











Frank Irwin

Berkeley, July, 1924

B. G. TEUBNER'S SAMMLUNG VON LEHRBÜCHERN
AUF DEM GEBIETE DER
MATHEMATISCHEN WISSENSCHAFTEN
MIT EINSCHLUSS IHRER ANWENDUNGEN.
BAND X 1.

NIEDERE ZAHLENTHEORIE

VON

PROF. DR. PAUL BACHMANN
ZU WEIMAR.

ERSTER TEIL.

LEIPZIG
DRUCK UND VERLAG VON B. G. TEUBNER
1902.

Vorrede.

Dies Buch verdankt seine Entstehung der ehrenden Aufforderung der B. G. Teubnerschen Verlagsanstalt, für ihr grofses Unternehmen, die Sammlung mathematischer Lehrbücher, ihr auch meinerseits einen Beitrag aus meiner Spezialwissenschaft, der Zahlentheorie, zu liefern. Längere Zeit habe ich gezögert, dieser Aufforderung nachzukommen, weil ich es für unthunlich hielt, neben meinem eigenen Versuche einer Gesamtdarstellung der Zahlentheorie in ihren Hauptteilen, ohne mich zu sehr zu wiederholen, noch ein besonderes Lehrbuch über einen Teil derselben zu schreiben; insonderheit schien für die „Niedere Zahlentheorie" die Gefahr einer Kollision dieser Art mit meinen „Elementen" sehr nahe zu liegen. Gleichwohl habe ich mich zur Ausarbeitung dieses Werkes entschlossen in der doppelten Erwägung, dafs einerseits ich dort bei der Beschränkung auf die „Hauptteile" der Wissenschaft d. i. auf diejenigen Gebiete derselben, welche den Grundstock ihres mächtigen Gebäudes ausmachen, so manches unberücksichtigt gelassen, was mehr als Anbau oder auch der Angliederung noch bedürftig anzusehen ist, andererseits, dafs der systematische Aufbau, den ich in den „Elementen" gewählt habe, sehr wohl — wenigstens in wesentlichen Punkten — durch einen andern ersetzt werden könne. So kann nun — meine ich — das vorliegende Werk, wenn es auch unvermeidlich in kleineren Partieen an die „Elemente" oder auch an andere bereits vorhandene Lehrbücher enger sich anschliefst, doch im Ganzen, nach Inhalt wie Begründung ein wesentlich davon verschiedenes, selbständiges genannt werden und dürfte als eine Art Supplementband meiner „Gesamtdarstellung" nicht unwillkommen sein. Dies wird vornehmlich gelten von dem ganzen zweiten Teile des Werkes, der diesem ersten baldmöglichst folgen und zum Unterschiede von der in ihm entwickelten multiplikativen d. h. auf den Begriff des Teilers begründeten Zahlentheorie die additive Zahlentheorie darstellen soll. Es gilt aber auch, von mannigfachen anderen Zuthaten abgesehen, vom 4. Kapitel dieses Teiles, dessen Gegenstand — die verschiedenen Euclidischen Algorithmen, die Fareyschen Reihen u. a. m. — in den „Elementen"

ganz übergangen ist, nicht minder von dem wesentlichsten Teile des 7. Kapitels, der Theorie der binomischen und allgemeineren Kongruenzen. Auch das 6. Kapitel, welches, zeitgemäfs einen Versuch Baumgart's erneuernd, die sämtlichen gegenwärtig bekannten Beweise des quadratischen Reziprozitätsgesetzes, soweit sie hierher gehören, in ihrem inneren Zusammenhange darstellt und mancherlei in engster Verbindung damit stehende Untersuchungen folgen läfst, wird wohl als neu befunden und vielleicht mit erhöhtem Interesse aufgenommen werden. Mit der Theorie der höheren Kongruenzen kann das Gebiet der „Niederen Zahlentheorie" überschritten scheinen. Dieser an sich überhaupt vage Titel ist jedoch für das Werk auch nur gewählt worden, um den Zusammenhang zu kennzeichnen, in welchem dasselbe, wie das gesamte Teubnersche Unternehmen mit der „Encyklopädie der mathematischen Wissenschaften", so im Besonderen mit deren gleichnamigem Artikel steht. Während aus diesem Zusammenhange es sich erklärt, dafs die Theorie der binären quadratischen Formen, die sonst zu den Elementen gerechnet zu werden pflegt, hier ganz ausgeblieben ist (übrigens wird der zweite Teil zu derselben nähere Stellung nehmen), ist die Theorie der höheren Kongruenzen noch in Betracht gezogen worden, um dem systematischen Bau des Werkes eine Art Krönung zu schaffen, ihn zu einer Höhe zu führen, von welcher aus mit dem siebenten Gaufsschen Beweise des Reziprozitätsgesetzes in die erhabneren Gebiete der Zahlentheorie ein reizvoller Blick sich eröffnet.

Weimar, den 28. November 1901.

Inhaltsverzeichnis.

Seite

Einleitung: Überblick über die Geschichte der Zahlentheorie . . 1—15
Pythagoras. Euclid. Diophantus. Die Inder. Die Araber. Leonardo von Pisa. Fermat. Leonhard Euler, Lagrange, Legendre. Gaufs' Disquisitiones arithmeticae. Die Zahlentheorie seit Gaufs . . . . 1—15

Erstes Kapitel: Die ganze Zahl und die einfachsten Rechnungsoperationen . . . . 16—29
Nr. 1. Mehrheit, Gesamtheit, Vielheit . . . . 16—18
Nr. 2. Die Ordinalzahlen 18
Nr. 3. Ähnliche Mehrheiten . . . . 18—19
Nr. 4. Endliche und unendliche Mehrheiten . . . . 19—20
Nr. 5. Abschnitte der Zahlenreihe; sie sind endliche Mehrheiten . . . 20—21
Nr. 6. Die Kardinalzahlen. Die Anzahl . . . . 21—22
Nr. 7. Addition und Subtraktion. Kleinste und gröfste Zahlen einer endlichen Mehrheit . . . . 23—25
Nr. 8. Multiplikation . . . . 25—26
Nr. 9. Negative Zahlen. Die Null . . . . 26—29

Zweites Kapitel: Von der Teilbarkeit der Zahlen . . . . 30—67
Nr. 1. Grundformel der Zahlentheorie. Brüche, Quotienten. Das gröfste Ganze $[x]$ . . . . 30—33
Nr. 2. Gemeinsame und der gröfste gemeinsame Teiler zweier Zahlen; relativ prime (teilerfremde) Zahlen. Modulus ganzer Zahlen. Die Euclidischen Fundamentalsätze von der Teilbarkeit . . . 33—36
Nr. 3. Die gemeinsamen und der gröfste gemeinsame Teiler mehrerer Zahlen. Zerlegung dreier Zahlen in ihre Kerne . . . . 36—37
Nr. 4. Die gemeinsamen und das kleinste gemeinsame Vielfache mehrerer Zahlen. Besonderer Fall von Zahlen, die zu je zweien teilerfremd sind. Satz von Lucas . . . . 38—40
Nr. 5. Zusammengesetzte und unzerlegbare Zahlen (Primzahlen). Hauptsatz: Zerlegung einer Zahl in Primzahlfaktoren . . . . 40—42
Nr. 6. Legendre's Satz zur Entscheidung, ob eine Zahl Primzahl sei. Das Sieb des Eratosthenes . . . . 42—43
Nr. 7. Es giebt unendlich viel Primzahlen (Euclid, Kummer). Dirichlet's Satz von der arithmetischen Progression; die Progression $6x - 1$ (Lucas). Unmöglichkeit der Gleichung
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p = a^m \pm b^m$ für $m > 1$ . . . . . 43—46
Nr. 8. Alle Teiler einer Zahl, deren Anzahl, Summe, Summe ihrer h^{ten} Potenzen. Die Anzahl der Zerlegungen einer Zahl in zwei (insbesondere teilerfremde) Faktoren . . . . 46—49
Nr. 9. Bestimmung des gröfsten gemeinsamen Teilers sowie des kleinsten gemeinsamen Vielfachen mehrerer Zahlen . . . . 49—50
Nr. 10. Die Faktoriellen. Bestimmung der höchsten darin aufgehenden Potenz p^ν einer Primzahl p . . . . 50—52
Nr. 11. Darstellung einer Zahl im Ziffernsysteme einer gegebenen Grundzahl. Beispiele: das dekadische System, die Grundzahlen 2 und 3. Legendre's Formel für ν . . . . 52—55

Seite

Nr. 12. Der Polynomial- insbesondere der Binomialkoeffizient . . . 55—57

Nr. 13. Der Bruch $\frac{(nq)!}{(q!)^n}$; Untersuchungen von Weill, André und de Polignac . . . . 57—62

Nr. 14. Sätze von Catalan und Bourguet . . . . 62—64

Nr. 15. Ihre Verallgemeinerung durch Landau . . . . 64—66

Nr. 16. Ein Satz von Liouville über das Produkt $m(m+1)\cdots(m+n-1)$ 66—67

Drittes Kapitel: Reste und Kongruenzen . . . . 67—99

Nr. 1. Kongruente Zahlen (Gaufs); Restklassen, Restsysteme (mod. n). Reduzierte Restsysteme. Die (Eulersche) Funktion $\varphi(n)$ . . 67—69

Nr. 2. Einfachste Kongruenzsätze . . . . 69—71

Nr. 3. Regeln für die Teilbarkeit einer (dekadischen) Zahl durch eine gegebene Zahl . . . . 71—73

Nr. 4. Lösungen und Wurzeln einer Kongruenz $f(x) \equiv 0$; ihr Grad; Anzahl ihrer Wurzeln für einen Primzahlmodulus . . . . . 73—75

Nr. 5. Auflösung der Kongruenz ersten Grades, Möglichkeitsbedingung, Anzahl der Wurzeln. Die Gleichung $ax + by = c$ . . . . 75—78

Nr. 6. Zerlegung eines Bruchs $\frac{m}{n}$ in Partialbrüche und in einfache Brüche . . . . 78—80

Nr. 7. Gleichzeitige Wurzeln mehrerer Kongruenzen $x \equiv \alpha \ (\text{mod.}\ a), \quad x \equiv \beta \ (\text{mod.}\ b), \cdots$ . . . . . 80—83

Nr. 8. Zweite Methode der Auflösung für den Fall teilerfremder Moduln. Jede Kongruenz ersten Grades kommt auf solche zurück, deren Moduln Primzahlen sind . . . . 83—86

Nr. 9. Herleitung der Formel $\varphi(mn) = \varphi(m)\varphi(n)$, falls m, n teilerfremd sind. Ausdruck von $\varphi(n)$ mittels der Primfaktoren von n. Veränderung der fundamentalen Formel, falls m, n nicht teilerfremd sind. . . . . 86—89

Nr. 10. Der Satz $\sum_d \varphi\left(\frac{n}{d}\right) = n$. Formel von Pepin und Moret-Blanc 89—91

Nr. 11. Verallgemeinerung von $\varphi(n)$ durch Schemmel und Lucas; die dann geltenden analogen Sätze. . . . . 91—94

Nr. 12. Allgemeiner Satz über die Verteilung der Teiler einer Zahl in zwei bestimmte Gruppen. Umkehrung der Beziehung $f(n) = \sum_d \psi(d)$ . . . . 94—97

Nr. 13. Determinante von St. Smith . . . . 97—99

Viertes Kapitel: Der Euclidische Algorithmus . . . . 99—153

Nr. 1. Der Euclidische Algorithmus als Quelle für die Fundamentalsätze von der Teilbarkeit . . . . 99—101

Nr. 2. Der aus ihm entspringende Kettenbruch, seine Näherungsbrüche, Bildungsgesetz ihrer Zähler und Nenner . . . . 101—104

Nr. 3. Die Gaufsischen Klammern . . . . 104—105

Nr. 4. Grund der Bezeichnung „Näherungsbrüche“ . . . . 105—107

Nr. 5. Weitere bezügliche Sätze. Die Gleichung $mx + ny = 1$ . . 107—109

Nr. 6. Symmetrische Kettenbrüche. Satz über Quadratsummen . . 109—112

Nr. 7. Modifizierte Euclidische Algorithmen und die ihnen entsprechenden Kettenbrüche. Für jeden irreduktibeln echten Bruch $\frac{m}{n}$ giebt es n Kettenbruchentwicklungen . . . . 112—114

Nr. 8 und 9. Ausdehnung der verschiedenen Algorithmen; Untersuchungen von Lamé, Binet, Dupré . . . . 114—118

Nr. 10. Binet's Algorithmus. Satz von Lambert über Zerlegung eines Bruchs in Stammbrüche . . . . 118—121

Nr. 11. Die Fareyschen Reihen verschiedener Ordnung. Sätze von Cauchy und Farey . . . . 121—125

Seite

Nr. 12. Die Näherungswerte einer Gröfse w; die, falls w irrational ist, unendliche Reihe der aufeinanderfolgenden; die Charakteristik (Christoffel, Hurwitz) und Grund dieser Bezeichnung . . . 125—128
Nr. 13. Zusammenhang zwischen der Charakteristik und dem gewöhnlichen Kettenbruche für w . . . . 128—130
Nr. 14. Die Charakteristiken äquivalenter Gröfsen . . . . 130—133
Nr. 15. Zusammenhang zwischen den Näherungswerten von w und den übrigen Kettenbruchentwicklungen . . . . 133—138
Nr. 16. Längste und kürzeste Kettenbruchentwicklungen . . . . . . 138—142
Nr. 17. Die Sternsche Entwicklung (r, s); Mittelglied, Stamm- und Summenglieder . . . . 142—143
Nr. 18. Die einfachste Entwicklung (1, 1) und ihre Eigenschaften . . 144—146
Nr. 19—21. Die daraus folgenden Eigenschaften von (r, s) . . . . 146—151
Nr. 22. Eine Eisensteinsche Funktion . . . . 151—153

Fünftes Kapitel: Die Sätze von Fermat und von Wilson . . . 153—179

Nr. 1. Der allgemeine Fermatsche Satz: $a^{\varphi(n)} \equiv 1 \pmod{n}$. Euler's Beweis des einfachen Satzes $a^{p-1} \equiv 1 \pmod{p}$ . . . . . . 153—154
Nr. 2. Lagrange's Beweis des letztern; Wilson's Satz . . . . 155—156
Nr. 3. Übergang vom einfachen zum allgemeinen Fermatschen Satze 156—158
Nr. 4. Wie der (einfache) Fermatsche Satz umzukehren ist (Lucas); 65537 ist Primzahl . . . . 158—159
Nr. 5. Untersuchung der durch die Kongruenz

$$a^{p-1} \equiv 1 + p \cdot q(a) \pmod{p^2}$$

definierten Zahl $q(a)$ durch Stern . . . . 159—162
Nr. 6. Spezialfall: der Rest von $\frac{2^{p-1}-1}{p} \pmod{p}$ . . . . 162—165
Nr. 7. Bestimmung von $q(a)$ nach Mirimanoff . . . . 165—169
Nr. 8. Der verallgemeinerte Wilsonsche Satz (Gaufs). Hilfsbetrachtung: Anzahl der Wurzeln von $x^2 \equiv 1 \pmod{n}$ . . . . . 170—172
Nr. 9. Beweis des allgemeinen Wilsonschen Satzes . . . . 172—174
Nr. 10. Er ist enthalten in einem Satze von Schemmel; Beweis eines Spezialfalls des letztern . . . . 174—175
Nr. 11. Ein bezüglicher Satz von Steiner . . . . 176—177
Nr. 12. Unmöglichkeit der Gleichung $1 \cdot 2 \cdot 3 \cdots (p-1) + 1 = p^k$, falls $p > 5$ (Liouville). Für $p = 4z + 3$ ist

$$1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \equiv \pm 1 \pmod{p};$$

Entscheidung über das Vorzeichen (Dirichlet). Ergänzung zu Kap. 2, Nr. 10: Rest von $\frac{n!}{p^{\nu}} \pmod{p}$, (Stickelberger) . . 177—179

Sechstes Kapitel: Die Theorie der quadratischen Reste . . . 180—318

Nr. 1. Die Kongruenz $ax^2 + bx + c \equiv 0 \pmod{n}$ kommt zurück auf $x^2 \equiv m \pmod{n}$. Bedingungen der Möglichkeit für die letztere, Anzahl ihrer Wurzeln . . . . 180—184
Nr. 2. Quadratische Reste und Nichtreste, die Anzahl derselben je $\frac{p-1}{2}$; die Symbole von Legendre und von Jacobi; ihre Eigenschaften . . . . 184—187
Nr. 3. Eulersches Kriterium von Schering verallgemeinert; neuer Beweis des Fermatschen Satzes . . . . 187—190
Nr. 4. Das Gaufssche Lemma und seine Verallgemeinerung durch Schering: $\left(\frac{Q}{P}\right) = (-1)^{\mu(Q,P)}$ . . . . 190—194
Nr. 5. Das Reziprozitätsgesetz und seine beiden Ergänzungssätze. Beweise des ersten Ergänzungssatzes . . . . 194—196
Nr. 6. Beweis des zweiten Ergänzungssatzes . . . . 196—197

Seite

Nr. 7. Ausdehnung der Ergänzungssätze auf das Jacobische Symbol; allgemeinster Ausdruck des Reziprozitätsgesetzes . . . . . 197—200

Nr. 8. Geschichtliches über Entdeckung und Beweis des Reziprozitätsgesetzes; chronologische Tabelle all' seiner bisherigen Beweise; ihre verschiedenen Kategorieen; die hier behandelten 200—206

Nr. 9. Der erste Gaufsische Beweis in Dirichlet's Darstellung; der Gaufsische Hilfssatz . . . . 206—212

Nr. 10. Hilfsbegriffe und Bezeichnungen (Kronecker): der Unterschied $R(x) = x - \left[x + \frac{1}{2}\right]$; $\text{sgn.}\, x = \frac{x}{|x|}$; die neue Form des verallgemeinerten Gaufsischen Lemma; die verschiedenen Ausdrücke des Reziprozitätsgesetzes . . . . 212—216

Nr. 11. Die fundamentalen Beziehungen

$$R(x+1) = R(x), \quad R(x) + R(-x) = 0.$$

Der fünfte Gaufsische Beweis . . . . 216—220

Nr. 12. Weitere Eigenschaft von $R(x)$: $\text{sgn.}\, R(x) = (-1)^{[2x]}$; die Kongruenz $\mu(Q, P) \equiv \sum_{h=1}^{\frac{P-1}{2}} \left[\frac{hQ}{P}\right]$ (mod. 2). Der dritte Gaufssche Beweis, seine geometrische Darstellung nach Eisenstein, seine Modifikation durch Voigt und Fields . . . . 220—227

Nr. 13. Genocchi's Beweis, seine ursprüngliche Quelle, seine arithmetische Grundlage; zwei interessante Summenformeln; wesentlich damit identisch ist Schering's Beweis. . . . . 228—233

Nr. 14. Kronecker's andere Formulierung der letzten zwei Beweise. Modifikation des Scheringschen auf Grund der Formel

$$\text{sgn.}\, R(x) = \text{sgn.} \prod_k (x-k)\left(x + \frac{1}{2} - k\right);$$

Herleitung der Formeln

$$\left(\frac{Q}{P}\right) = \text{sgn.} \prod_{h,k} \left(\frac{h}{P} - \frac{k}{Q}\right) \cdot \left(\frac{h}{P} + \frac{k}{Q} - \frac{1}{2}\right) = \text{sgn.} \prod_{h,k} \left(\frac{k}{Q} - \frac{h}{P}\right).$$

Diese folgen auch unmittelbar aus Gaufs' Bestimmung für $\text{sgn.}\, R(x)$ mittels der Formel $(-1)^{[2x]} = \text{sgn.} \prod_i (i - 2x)$. . 233—237

Nr. 15. Auf der gleichen Formel beruht schon Schaar's Beweis, dem sich die Beweise Gegenbauer's wie der von Lucas anreihen 237—242

Nr. 16. Einfachste Gestalt des dritten Gaufsischen Beweises (Kronecker). Bemerkungen von Schering. Verhältnis jenes Beweises zu denjenigen von Genocchi und Schering (logarithmische Umgestaltung) . . . . 242—245

Nr. 17. Kronecker's Beweis (auch Hermes') „durch Umkehrung" . . 245—249

Nr. 18. Busche's erster Beweis auf Grund eines allgemeinen arithmetischen Satzes . . . . 249—254

Nr. 19. Busche's zweiter Beweis auf Grund des modifizierten Gaufsschen Lemma. . . . . 254—256

Nr. 20. Lange's Beweise, denen wieder eine neue Modifikation desselben zu Grunde liegt . . . . 256—261

Nr. 21. Zwei weitere Eigenschaften der Funktion $R(x)$, deren die Beweise von Zeller und von Petersen bedürfen; Darstellung des ersteren . . . . 261—265

Nr. 22. Der Beweis von Petersen, auf einer anderen Form des Gaufsschen Lemma begründet. Modifizierter Kroneckerscher Beweis. Neue Ableitung des zweiten Ergänzungssatzes. . . . . . . 266—269

Seite

Nr. 23. Beweis von Bouniakowsky; erster Beweis von Schmidt . . . 270—274
Nr. 24. Zweiter Beweis von Schmidt eine Modifikation des fünften Gaufsischen . . . . 274—277
Nr. 25. Dritter Beweis von Schmidt . . . . 277—280
Nr. 26. Hilfssatz von Zolotareff, seine Verallgemeinerung durch Lerch. Beweis von Zolotareff . . . . 280—286
Nr. 27. Arithmetische Reihen, welche die Zahlen m liefern, für welche $\left(\frac{m}{n}\right)$ einen bestimmten Wert hat. Primteiler der Form $x^2 - my^2$ 286—290
Nr. 28 und 29. Direkte Wertbestimmung von $\left(\frac{m}{n}\right)$: 1) nach Gaufs auf Grund des gewöhnlichen Euclidischen Algorithmus, Untersuchungen von Zeller und Schering; 2) nach den Regeln von Eisenstein, Lebesgue, Kronecker, Sylvester, Gegenbauer . . 290—300
Nr. 30. Verteilung der quadratischen Reste und Nichtreste im Intervalle 0, p . . . . 300—306
Nr. 31. Die trigonalen und bitrigonalen Reste . . . . 306—311
Nr. 32 und 33. Beziehungen zwischen Summen quadratischer, trigonaler und bitrigonaler Reste oder Nichtreste . . . . 311—318

Siebentes Kapitel: Die höheren Kongruenzen . . . . 318—399

Nr. 1. Die binomische Kongruenz $x^m \equiv a \pmod{n}$ zurückgeführt auf $z^m \equiv 1 \pmod{n}$. Exponent, zu welchem eine Zahl (mod. n) gehört. Neuer Beweis des Fermatschen Satzes . . . . . . 318—322
Nr. 2. Primitive Wurzeln. Existenz primitiver Wurzeln (mod. p); ihre Anzahl . . . . 322—324
Nr. 3. Andere Herleitung derselben Resultate . . . . 324—327
Nr. 4. Existenz primitiver Wurzeln (mod. p^α); ihre Anzahl . . . . 327—330
Nr. 5. Die Moduln $n = 2$, $n = 4$. Für den Modulus $n = 2^\lambda$ $(\lambda > 2)$ giebt es keine primitive Wurzeln (mod. n), aber primitive Lösungen von $z^{2^{\lambda-2}} \equiv 1 \pmod{2^\lambda}$, z. B. $z = 5$ . . . . . . 331—333
Nr. 6. Sätze über Produkt und Summe aller (mod. p^α, $2p^\alpha$) zu gleichem Exponenten gehörigen Zahlen . . . . 333—336
Nr. 7. Neuer Beweis des allgemeinen Wilsonschen Satzes. . . . . 336—338
Nr. 8. Theorie der Indices (mod. n) . . . . 338—341
Nr. 9. Methoden zur Ermittlung einer primitiven Wurzel (mod. p) 341—343
Nr. 10. Potenzreste m^{ten} Grades (mod. p^α), charakteristische Bedingung für dieselben. Sätze über Summe und Produkt aller m^{ten} Potenzreste. Auflösung der Kongruenz $x^m \equiv a \pmod{p^\alpha}$. . . 343—348
Nr. 11. Die m^{ten} Potenzreste (mod. 2^λ) . . . . 348—351
Nr. 12. Entwicklung irreduktibler echter Brüche $\frac{r}{n}$ nach den negativen Potenzen einer Grundzahl g; insbesondere in Dezimalbrüche . . . . 351—354
Nr. 13. Ihre Periodizität; Länge der Periode . . . . 355—357
Nr. 14. Anwendung auf Dezimalbrüche. . . . . 357—359
Nr. 15. Satz über die Ziffern der Zahl $\frac{g^{\varphi(n)} - 1}{n}$ . . . . 359—361
Nr. 16. Beziehung zwischen den Entwicklungen von $\frac{r}{n}$, welche zwei (mod. n) kongruenten oder associierten Grundzahlen entsprechen . . . . 361—363
Nr. 17. Die allgemeine Kongruenz $f(x) \equiv 0 \pmod{n}$; n wird als Primzahl p vorausgesetzt. Grad von $f(x)$, Grad eines Produktes. Satz über Teilbarkeit eines Produktes durch p. Zerlegbarkeit von $f(x)$ (mod. p) in Faktoren, und Wurzeln von $f(x)$ . . . 363—366

Seite

Nr. 18. Kongruenz von Funktionen (mod. p); inkongruente Klassen primärer Funktionen m^{ten} Grades und deren Anzahl. Teiler von $f(x)$ (mod. p), irreduktible oder Primfunktionen . . . . 366—368

Nr. 19. Gröfster gemeinsamer Teiler zweier Funktionen (mod. p); relativ prime Funktionen. Fundamentalsätze von der Teilbarkeit der Funktionen (mod. p). . . . . 368—370

Nr. 20. Möglichkeit der Zerlegung einer Funktion in Primfunktionen (mod. p). Über gemeinsame Teiler einer Funktion und ihrer Ableitung . . . . 370—372

Nr. 21. Ermittlung der Anzahl (m) inkongruenter primärer Primfunktionen m^{ten} Grades nach Gaufs . . . . 372—375

Nr. 22. Kongruenz von Funktionen nach dem Doppelmodulus p, $P(x)$; Anzahl der inkongruenten Funktionen. Reduziertes Restsystem. Analogon des Fermatschen Satzes; die Kongruenz

$$X^{p^m} \equiv X \text{ (modd. } p,\ P(x))$$

hat p^m Wurzeln. Allgemeiner Satz über die Anzahl Wurzeln einer Kongruenz. Analogon des Wilsonschen Satzes . . . . 375—378

Nr. 23. Zerlegung der Funktion $x^{p^m} - x$ in Primfunktionen (mod. p). Neue Herleitung der Anzahl (m). Ausdruck für das Produkt aller Primfunktionen m^{ten} Grades . . . . 378—382

Nr. 24. Ermittlung der Primteiler einer gegebenen Funktion . . . . 382—383

Nr. 25. Exponent, zu welchem eine Funktion (modd. p, $P(x)$) gehört; Anzahl derjenigen Funktionen, die zu einem bestimmten Exponenten gehören . . . . 384—385

Nr. 26. Zerlegung von $x^\delta - 1$ in Primfaktoren (mod. p). Sätze über die Zerlegung von $\frac{x^q - 1}{x - 1}$, wenn q eine von p verschiedene Primzahl ist . . . . 385—388

Nr. 27. Exponent μ, zu welchem eine Funktion (modd. p, $P(x)$) pafst. Die zu μ passenden sind die Wurzeln der irreduktibeln Kongruenzen $P_\mu(x) \equiv 0$ (modd. p, $P(x)$) vom Grade μ. Ihre Anzahl ist $\mu \cdot (\mu)$. Es giebt stets Primfunktionen $P(x)$ so beschaffen, dafs eine Kongruenz n^{ten} Grades $F(X) \equiv 0$ (modd. p, $P(x)$) genau n Wurzeln hat . . . . 388—394

Nr. 28. Die Galoisschen Imaginären . . . . 394—396

Nr. 29. Gaufs' siebenter Beweis des Reziprozitätsgesetzes . . . . . 396—399

Zusätze . . . . 400—402

Druckfehler-Verzeichnis.

Seite 9 Zeile 4: lies „délectables" statt „delectables".
„ 31 „ 10 v. u.: lies „folgende:" statt „folgende;".
„ 58 „ 17: lies „$q \gtreqless 1$" statt „$q > 1$".
„ 113 „ 6: lies „$-\varepsilon_i \nu_i$" statt „$\varepsilon_i \nu_i$".
„ 114 „ 8 v. u.: „ „ „
„ 117 „ 11: „ „ „
„ 148 „ 20: lies „müfsten" statt „müfste".
„ 175 „ 4: lies „$n = abc\ldots$" statt „$abc\ldots$".
„ 209 „ 13 v. u.: lies „Rest von q" statt „Rest von p".
„ 222 letzte Zeile: lies „für $n = 0, 1, 2, \cdots \frac{Q-3}{2}$" statt „für $n = 1, 2, \cdots \frac{Q-3}{2}$".
„ 226 Zeile 5 fehlt zum Schlusse „ist".
„ 228 „ 4 v. u.: lies „$hQ + kP$" statt „$hQ + kQ$".
„ 336 „ 1: lies „die Summe" statt „die Summen".
„ 380 „ 3 v. u.: lies „$=$" statt „$\equiv$".

Gerade hundert Jahre sind verflossen, seit die Zahlentheorie, deren einfachere Teile hier ihre Darstellung finden sollen, als Wissenschaft geboren, in den ewig denkwürdigen *Disquisitiones Arithmeticae* von C. F. Gaufs (Lipsiae 1801) zum ersten Male als festgegründetes, die wesentlichsten Gebiete arithmetischer Probleme umfassendes, systematisch zusammenhängendes Ganzes aufgebaut worden ist.

Freilich sind die Zahlen, dieser ursprünglichste mathematische Begriff, schon von den frühesten Zeiten an dem Menschengeschlechte unentbehrlich und daher auch der älteste Gegenstand mathematischer Betrachtung gewesen. Die frühesten Dokumente der letzteren liegen uns in den Zahlwörtern vor als Zeugen von der Art und Weise, wie die verschiedensten Völker ihre Zahlensysteme gebildet d. h. die Reihe der Zahlen mittels einer besonderen Grundzahl in verschiedene Stufen, wie Einer, Zehner, Hunderter, geordnet haben. Mannigfach unterschieden sie sich hierbei in der Wahl dieser Grundzahl. Während zumeist nach der Anzahl der Finger einer Hand oder beider Hände die Fünf oder die Zehn dafür erwählt wurde, legten andere Völkerschaften an ihrer Statt die Zahl 20, worauf z. B. französische Zahlwörter wie quatre vingt zurückweisen, noch andere, wie die Babylonier, die Zahlen 6 oder 12 zu Grunde, aus deren Vermischung mit dem dekadischen Systeme dann das Sexagesimalsystem entsprang, dessen Spuren uns in der astronomischen Teilung der Grade in 60 Minuten, der letzteren in 60 Sekunden verblieben sind; der Zählung der Neuseeländer lag auffälliger Weise sogar die Zahl 11, eine Primzahl, zu Grunde. Mit dieser Bildung der Zahlensysteme war zugleich der Gebrauch der einfachsten Rechnungsoperationen, der Addition und der Multiplikation, bei einigen derselben, wie bei den römischen Zahlwörtern undecentum, duodeviginti, auch der der Subtraktion, teilweise auch, wie in den anderen: sequialter, *ἐπιδευτερος* (unserm anderthalb) u. s. w. derjenige der Division konstatiert. Die Bedürfnisse des Lebens und des Verkehrs erweiterten allgemach den Umfang und förderten eine eigene Kunst des Rechnens, die allen Angaben nach zuerst bei den Chaldäern eine entwickeltere gewesen, von ihnen den Babyloniern und von diesen wieder den Ägyptern vermittelt worden sein dürfte. Hier finden wir dann in dem Rechenbuche des Ahmes, der unter dem Hyksoskönige Apophis (zwischen 2000 und 1700 v. Chr.) gelebt

hat, die erste Darstellung der bereits aufgefundenen Regeln, teils für die Rechnung mit Brüchen, teils solche zur Auflösung von Aufgaben, die nach unserer Ausdrucksweise auf Gleichungen ersten Grades mit einer Unbekannten zurückkommen. Allmählich traten zu derartigen Aufgaben auch die Auflösung von Gleichungen zweiten Grades hinzu, die Aufgabe der Quadrat- und der Kubikwurzelausziehung u. dgl., und schon war in der Quadratwurzel aus 2 selbst der Begriff des Irrationalen dem Pythagoras (etwa um 540 v. Chr.) und seiner Schule nicht mehr fremd.

Aber all' diese arithmetischen Operationen und Regeln, um gegebene Zahlen mit einander zu verknüpfen oder aus solchen eine Unbekannte zu finden, waren noch keine Zahlentheorie. Diese beginnt erst, wo die Zahl selbst mit ihren spezifischen Eigenschaften Gegenstand der Betrachtung wird. In der Geschichte der Mathematik finden wir dies zuerst bei Pythagoras, der somit als Vater der Zahlentheorie bezeichnet werden kann. Da er selbst und seine Schüler schriftliche Zeugnisse der ihnen bekannten Zahlenlehre nicht hinterlassen haben, sind wir für unsere Kenntnis derselben auf die Mitteilungen angewiesen, welche spätere Schriftsteller darüber gemacht haben, unter ihnen vornehmlich Proklus Diadochus (5. Jhdt. n. Chr.), der Herausgeber eines sehr wichtigen Bruchstückes eines älteren Schriftstellers, wahrscheinlich des Eudemos, sodann in seiner „Einleitung in die Arithmetik“ Nikomachus (um 100 n. Chr.) und Jamblichus (Anfang des 4. Jhdt. n. Chr.), welcher zu der letzteren Erläuterungen gegeben hat. Nach diesen Gewährsmännern war den Pythagoräern nicht nur der Unterschied gerader und ungerader Zahlen, sondern auch der Begriff der Primzahl geläufig, wenngleich sie die ganze Bedeutsamkeit des letztern nicht gekannt zu haben scheinen. Die Einheit war ihnen, wie auch lange noch später, zwar Ursprung aller Zahlen, da diese aus der additiven Verknüpfung von Einheiten hervorgehen, nicht aber selbst eine Zahl. Natürlicherweise waren die ersten allgemeinen Beziehungen, die man zwischen Zahlen auffand, additiver Natur, wie diejenigen, die wir in den Formeln

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2},$$
$$1 + 3 + 5 + \cdots + (2n-1) = n^2$$

aussprechen; sie führten die Pythagoräer zur Kenntnis der sogenannten Dreiecks- und Quadratzahlen, der beiden einfachsten Arten der Polygonalzahlen, deren allgemeine Definition aber den Pythagoräern noch nicht, sondern frühestens dem Hypsikles von Alexandrien (etwa um 180 v. Chr.) bekannt gewesen sein dürfte. Nach Plutarch (1. Jhdt. n. Chr.) wären dagegen Jene mit dem in der Formel

$$8 \cdot \frac{n(n+1)}{2} + 1 = (2n+1)^2$$

enthaltenen Satze, nach Theon von Smyrna (um 130 n. Chr.) mit dem Satze

$$n^2 + (2n+1) = (n+1)^2$$

der Sache nach schon bekannt gewesen, während Nikomachus des andern Satzes erwähnt, nach welchem die Summe zweier aufeinanderfolgender Dreieckszahlen eine Quadratzahl ist:

$$\frac{n(n-1)}{2} + \frac{(n+1)n}{2} = n^2.$$

Bei Theon von Smyrna ist zudem eine Reihe von Zahlen α_n, β_n, die als Seiten- und Diagonalzahlen bezeichnet und nach den Formeln

$$\alpha_{n-1} + \beta_{n-1} = \alpha_n, \quad 2\alpha_{n-1} + \beta_{n-1} = \beta_n$$

gebildet werden (Nenner und Zähler der Näherungsbrüche des Kettenbruchs für $\sqrt{2}$), als frühestes Beispiel rekurrenter Zahlenreihen sehr bemerkenswert.

Verbanden sich schon mit diesen Gattungen von Zahlen geometrische Vorstellungen und Beziehungen, so führten die Untersuchungen des Pythagoras über das Dreieck ihn zu einer anderen Reihe besonderer Zahlen und in ein neues Gebiet der Zahlenlehre hinein. Sei es, daſs der berühmte Satz vom Quadrat der Hypotenuse eines rechtwinkligen Dreiecks Ausgangspunkt oder Folge davon gewesen sei, gewiſs ist der Umstand, daſs dem Pythagoras die ausgezeichnete Eigenschaft der drei aufeinanderfolgenden Zahlen 3, 4, 5 bekannt gewesen, nach welcher $3^2 + 4^2 = 5^2$ ist und kraft deren drei Längen von der Gröſse dieser Zahlen geeignet sind, indem man aus ihnen ein Dreieck bildet, einen rechten Winkel zu konstruieren, eine Methode, welche (nach Biernatzki, Journ. f. Math. 52, p. 59) bereits den alten Chinesen bekannt gewesen, von Vitruv in seiner „Architektur“ (14 n. Chr.) den Bauleuten gelehrt worden und noch heutigen Tags bei diesen in Anwendung ist. Für die Aufgabe nun, andere Zahlen dieser Art, welche den Namen „Pythagoräische Zahlen“ erhalten haben, unter denen übrigens die Zahlen 3, 4, 5 die einzigen sind, die zu dreien aufeinanderfolgen, für die Aufgabe also, rechtwinklige Dreiecke zu finden, deren Seiten ganzzahlige Werte haben, hat nach des Proklus' Zeugnis ebenfalls Pythagoras selbst schon eine Regel gegeben, die sich in unserer Schreibweise durch die Identität

$$(2n+1)^2 + (2n^2+2n)^2 = (2n^2+2n+1)^2$$

ausdrücken läſst. Plato (430—347 v. Chr.) setzte an ihre Stelle die andere:

$$(2n)^2 + (n^2-1)^2 = (n^2+1)^2.$$

Nun stellt sich der additiven Bildung der Zahlen, die auch bei diesen letzteren Sätzen der Pythagoräischen Schule im Vorder-

grunde steht, eine andere gegenüber, die **multiplikative**, insofern eine Zahl als Vielfaches einer anderen, diese als Teiler der ersteren gedacht wird. Zwar läſst sich ein Vielfaches von n auch additiv bilden als Summe einer gewissen Anzahl gleicher Zahlen n und erscheint so nur als eine besondere Gattung additiv gebildeter Zahlen. Aber, indem das Produkt dieser Operation eine Zahl ist, welche aus der Zahl n, dem Multiplikanden, auf dieselbe Weise hervorgeht, wie eine andere Zahl, der Multiplikator, aus der Einheit, wird hier die Bildung der Zahlen auf eine höhere Stufe gehoben, in einen umfassenderen Gesichtspunkt gerückt derart, daſs nun umgekehrt die additive Entstehung einer Zahl aus der Einheit wieder nur zu einem besonderen Falle der Produktbildung wird. Der erste Mathematiker, der in ausgiebigerer Weise diese multiplikative Bildung der Zahlen verfolgte, war **Euclid** (um 300 n. Chr., unter der Regierung des ersten Ptolemäers, in Alexandria lebend). Das Hauptwerk dieses Schriftstellers, die Elemente (στοιχεῖα) des **Euclid**, welche die Jahrhunderte hindurch bis in die neuere Zeit hinein unentwegte Grundlage der Geometrie gewesen und auch noch in der Gegenwart diejenige des geometrischen Schulunterrichts geblieben sind, handelt zwar vorwiegend von der Geometrie, enthält aber in seinem 7., 8., 9. Buche als eine für die Zwecke derselben bestimmte Einschaltung und zumeist auch in geometrischer Einkleidung eine Reihe mathematischer Untersuchungen, in denen wir die ersten festen Grundlagen der heutigen Zahlentheorie zu erblicken haben. Inwieweit die darin gegebenen Sätze das geistige Eigentum **Euclids** sind, läſst sich kaum mehr ermitteln; nach **Proklus'** Angabe, daſs „**Euclid**, der die Elemente zusammenstellte, vieles von **Eudoxus** Herrührende zu einem Ganzen ordnete, vieles von **Theaetet** Begonnene zu Ende führte, überdies das von den Vorgängern nur leichthin Bewiesene auf unwiderlegliche Beweise stützte", hat man jedenfalls die Elemente als eine in selbständigem Denken und eigener geistiger Arbeit erfaſste Systematisierung des bis dahin Bekannten zu betrachten und einzuschätzen. Was insbesondere die zahlentheoretischen Teile betrifft, so ist der Fortschritt, den sie gegen die Vorzeit bezeigen, bereits im Allgemeinen charakterisiert; im Besonderen ist noch zu erwähnen, daſs **Euclid** hier auf Grund des Begriffs eines gemeinsamen Teilers zweier Zahlen, welch' letztern er ganz durch den Algorithmus bestimmt, der auch heut noch dazu verwendet und als **Euclidischer** Algorithmus benannt wird, die fundamentalsten Sätze über die Teilbarkeit der Zahlen begründet, so auch die unendliche Menge der Primzahlen bewiesen, daſs er ferner die Summierung der geometrischen Reihe vollzogen, die allgemeine Formel für die Pythagoräischen Zahlen gegeben und eine bis dahin kaum schon betrachtete Gattung von Zahlen, die der „vollkommenen" Zahlen näher untersucht hat; in

Bezug auf die letztern, diejenigen Zahlen nämlich, deren aliquote Teile in Summa ihnen selbst gleich sind, gab er eine allgemeine Bildungsregel, die auch heut noch nicht überboten und vervollständigt ist.

Anderes übergehend sei hier im Anschlufs an Euclid nur noch der unter dem Namen des *„Siebes, cribrum“* des (276 in Kyrene geborenen) Eratosthenes bekannt gewordenen Methode, um aus der Zahlenreihe die Reihe der Primzahlen auszuscheiden, desgleichen eines bemerkenswerten Satzes gedacht, der zuerst in des Nikomachus von Gerasa *„Einleitung in die Arithmetik“* erwähnt wird, eines Satzes, welcher in den Gleichheiten $2^3 = 3 + 5$, $3^3 = 7 + 9 + 11$ u. s. w. zu Tage tritt und durch die allgemeine Formel

$$n^3 = (n^2 - n + 1) + (n^2 - n + 3) + \cdots + (n^2 - n + (2n - 1))$$

bestätigt wird.

Der nächste arithmetische Schriftsteller, dessen Werke für die Geschichte der Zahlentheorie von Wichtigkeit sind, ist Diophantus von Alexandrien (um 350 n. Chr. unter Kaiser Julian), von welchem sechs seiner dreizehn Bücher *„Arithmetica“* und ein paar kleinere Schriften, darunter eine über Polygonalzahlen, auf uns gekommen sind. Seine Bedeutung ruht dabei weniger in dem, was er selbst gefunden, als in dem, was er gewirkt hat und was spätere Forscher an ihn geknüpft haben. Aber auch in seinen eigenen Resultaten ist die Erschliefsung eines neuen arithmetischen Gebiets anzuerkennen, dessen Ausbeutung nun zunächst für längere Zeit die zahlentheoretische Forschung beherrscht. Was Diophant gegeben hat, sind in erster Linie wieder numerische Auflösungen bestimmter Gleichungen ersten oder höheren Grades, gehört also der Zahlentheorie nicht an; weiterhin Sätze, welche, obwohl sie Deutungen gestatten, die zahlentheoretisch interessieren, doch ihrem Wesen nach algebraische Identitäten sind, u. a. die folgenden drei:

der Satz, dafs in jedem rechtwinkligen Dreiecke das Quadrat der Hypotenuse auch dann noch ein Quadrat bleibe, wenn man das Doppelte des aus den Katheten gebildeten Rechtecks dazufügt oder davon hinwegnimmt, in algebraischen Zeichen:

$$(a^2 + b^2) \pm 2ab = (a \pm b)^2;$$

ferner, dafs das Produkt aus der Summe zweier Quadrate in eine ebensolche Summe auf zwiefache Weise wieder eine solche sei, nämlich

$$(a^2 + b^2)(a'^2 + b'^2) = (ab' \pm a'b)^2 + (aa' \mp bb')^2;$$

endlich, dafs jede Quadratzahl auf beliebig viel Weisen Summe zweier Quadratzahlen sei nach der Formel:

$$a^2 = \left(\frac{2m}{m^2+1}\,a\right)^2 + \left(\frac{m^2-1}{m^2+1}\,a\right)^2.$$

Aber auch eigentlich zahlentheoretische Sätze und Aufgaben finden sich vor, z. B. der bedeutsame Satz, dafs keine Zahl von der Form $4n + 3$ eine Summe zweier Quadratzahlen sein könne, desgleichen in seiner Abhandlung von den Polygonalzahlen die Frage, auf wieviel verschiedene Weisen eine Zahl Polygonalzahl sei u. s. w. Woran man aber beim Namen Diophant am meisten zu denken hat, weil es, wenn auch Spuren davon schon früher, z. B. in den Pythagoräischen Zahlen, zu finden sind, doch vorzugsweise ihm eigentümlich ist, das ist die sogenannte „Unbestimmte Analysis", die Aufgabe, eine Gleichung mit mehr als einer Unbekannten, mithin zu eindeutig bestimmter Ermittelung der letzteren nicht genügend, zu lösen. Eine gröfsere Reihe derartiger Aufgaben vornehmlich ersten Grades und von gröfserem oder geringerem Interesse hat Diophant mit vielem Scharfsinn und einer virtuosen Gewandtheit gelöst; zwiefach aber blieb seine Kunst doch mangelhaft, einmal, insofern sie allgemeiner Methoden entbehrte, seine Probleme zu bewältigen, andererseits, insofern sie sich mit deren Lösung in rationalen Zahlen begnügte, die schwierigere Lösung in ganzen Zahlen bei Seite setzend. Durch letzteren Umstand allein schon wird, ganz abgesehen davon, dafs ein wirklich zahlentheoretisches Interesse der unbestimmten Analysis nur bedingungsweise zukommt, die Bedeutung Diophants für die Zahlentheorie sehr erheblich gemindert.

In der angegebenen Beziehung sind dem Diophant die indischen Arithmetiker, soweit wir von ihnen wissen, Aryabhatta (geb. 476 n. Chr.), Brahmagupta (598) in seinem *„verbesserten Systeme des Brahma"*, und besonders Bhaskara Acarya (der Gelehrte, geb. 1114) in seiner *„Krönung des Systems"* entschieden überlegen. Ihre Zahlentheorie bewegt sich hauptsächlich ebenfalls im Gebiete der unbestimmten Analysis, aber im Unterschiede zu Diophant werden meist ganzzahlige Lösungen verlangt. Auch handelt es sich neben Gleichungen ersten Grades schon um solche des zweiten, unter denen vornehmlich die Gleichung $ax^2 + b = cy^2$ unser Interesse beansprucht. Hier bemerke man die eigentümliche „cyklische" Methode, durch welche Bhaskara die Lösung der besonderen derartigen Gleichung $ax^2 + 1 = y^2$ sucht. Ausgehend von ganzen Zahlen A, B, C, welche die Bedingung $aA^2 + B = C^2$ erfüllen, sucht er andere Zahlen A_1, B_1, C_1, zwischen denen die analoge Beziehung $aA_1^2 + B_1 = C_1^2$ besteht, u. s. w., bis er — was freilich nur eventuell eintreffen wird — auf eine ganzzahlige Lösung der vorgelegten Gleichung geführt wird. Als rationale Lösung derselben werden die Ausdrücke

$$x = \frac{2AC}{B}, \quad y = \frac{aA^2 + C^2}{B}$$

von Bhaskara aufgestellt. Mit besonderer Vorliebe verweilen diese indischen Arithmetiker bei der Bildung rationaler Dreiecke und Vierecke

d. i. bei der Aufgabe, solche Figuren zu bilden, deren Seiten (und Diagonalen) zugleich mit ihrem Inhalte ganzzahlige Werte haben, einer Verallgemeinerung also der schon von Pythagoras behandelten Aufgabe von rechtwinkligen Dreiecken gleicher Beschaffenheit.

Die Araber, welche nun als Erben der indischen Arithmetiker in die Geschichte der Mathematik eintreten, bewegen sich, was ihre Zahlentheorie betrifft, ungefähr in den gleichen Kreisen, wie jene; ihr Verdienst um diese Wissenschaft besteht weniger in den Resultaten, die sie gefunden, als in dem ausgezeichneten Rüstzeuge, das sie zu weiteren Funden, wie der gesamten Mathematik, so auch ihr einerseits mit dem dekadischen Ziffernsysteme, andererseits mit der Buchstabenrechnung verschafft haben. An neuen zahlentheoretischen Ergebnissen heben wir die Betrachtung der „befreundeten Zahlen“ d. i. je zwei solcher Zahlen, deren aliquote Teile in Summa je der anderen gleich sind, und die Vorschrift des Tabit ibn Kurra (826—901) hervor, solche Paare zu finden; in ersichtlichem Anschlufs an Euclids Regel zur Bildung vollkommener Zahlen sagt sie aus, dafs, wenn

$$p = 3 \cdot 2^n - 1, \quad q = 3 \cdot 2^{n-1} - 1, \quad r = 9 \cdot 2^{2n-1} - 1$$

Primzahlen sind, $A = 2^n pq$, $B = 2^n r$ zwei befreundete Zahlen sein werden. Ferner die schon den römischen Agrimensoren bekannte Beziehung

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2,$$

für welche Alkarchi (um 1010) einen sehr anschaulichen Beweis gab, die Summierung auch der vierten Potenzen aufeinanderfolgender Zahlen, u. dgl. Im übrigen handelt es sich auch hier um unbestimmte Gleichungen teils in Verbindung mit der Theorie der rationalen rechtwinkligen Dreiecke, wie z. B. um den schon jetzt bemerkten Satz, dafs die Summe zweier Kubikzahlen nie wieder eine Kubikzahl sei, teils, wie bei Beha-Eddin (1547—1622) um Gleichungen neuer Art, deren Unmöglichkeit behauptet wird, wie die folgende:

$$x^2 \pm 10 = y^2,$$

u. a.

Die Mathematik der abendländischen Völker, bis dahin fast ganz in dem Umfange verharrend, welcher dieser Wissenschaft durch die Arbeiten der griechischen und lateinischen Forscher gegeben worden war, empfing nunmehr von der arabischen Wissenschaft neue Triebkraft, die auch für die Zahlentheorie allmählich fruchtbringend wurde. Gleichwohl ist in einem Zeitraume mehrerer Jahrhunderte nur wenig von Belang für diese Wissenschaft zu verzeichnen. Das bei weitem Wichtigste davon ist das, im Jahre 1228 in zweiter Auflage erschienene *liber Abaci* des Leonardo von Pisa (auch Fibonacci = filio di Bonaccio genannt). Dies vorzügliche „die Methode der

Inder enger umfassende, Eigenes hinzufügende und manches von den Feinheiten der geometrischen Kunst des Euclid beisetzende" sehr beachtenswerte und reichhaltige Werk enthält in der That auch mehreres, was zahlentheoretisch von Wert war bezw. noch ist. Dahin zählt die Auflösung der Gleichung $x^2 + y^2 = a^2$ in rationalen Zahlen, namentlich aber die (bei der sogenannten Kaninchen-Aufgabe auftretende) nach der Formel $u_{n+1} = u_n + u_{n-1}$ gebildete „Zahlenreihe von Fibonacci". In einer andern Schrift, der *pratica geometriae* (1220) behandelt derselbe Schriftsteller die unbestimmte Gleichung $x^2 + a = y^2$; indem er sich daran erinnert, dafs die Summe aufeinanderfolgender ungerader Zahlen eine Quadratzahl sei, findet er für ein ungerades $a = 2n + 1$ die Lösung $x = n$, $y = n + 1$, für eine durch 4 teilbare Zahl $a = (2n - 1) + (2n + 1)$ die Lösung $x = n - 1$, $y = n + 1$; für eine nur durch 2 teilbare Zahl a ist die Gleichung nicht lösbar. Die Verallgemeinerung dieser Aufgabe führt zu der anderen, im *liber quadratorum* (1225) behandelten Aufgabe, drei in arithmetischer Progression folgende Quadratzahlen x^2, y^2, z^2, für welche also $x^2 - y^2 = y^2 - z^2$ ist, zu ermitteln. Heifst a der gemeinsame Wert beider Differenzen, so nennt Leonardo die hier zulässigen Zahlen a die numeri congrui; die Aufgabe kommt auf die andere zurück, für jede solche Zahl die beiden Gleichungen

$$x^2 = y^2 + a, \quad z^2 = y^2 - a$$

zu erfüllen; sie löst sich nach der schon den Arabern bekannten algebraischen Identität

$$(\alpha^2 + \beta^2)^2 \pm 4\alpha\beta(\alpha^2 - \beta^2) = (\alpha^2 - \beta^2 \pm 2\alpha\beta)^2,$$

welche im Ausdrucke $4\alpha\beta(\alpha^2 - \beta^2)$ die allgemeine Form der numeri congrui und für jede solche Zahl als die gesuchten Quadratzahlen

$$x = \alpha^2 - \beta^2 + 2\alpha\beta, \quad y = \alpha^2 + \beta^2, \quad z = \alpha^2 - \beta^2 - 2\alpha\beta$$

liefert; Leonardo, der übrigens die Aufgabe auf andere Weise behandelt, beweist, dafs, jenachdem $\alpha + \beta$ gerade oder ungerade ist, der erste bezw. zweite der Ausdrücke

$$\alpha\beta(\alpha^2 - \beta^2), \quad 4\alpha\beta(\alpha^2 - \beta^2)$$

und somit jederzeit die numeri congrui durch 24 teilbar sind.

Vier Jahrhunderte lang ruhte nun die Zahlentheorie, wenn wir etwa die für die Teiler 1 bis 10 aufgestellten Teilbarkeitsregeln des Michael Stifel (geb. 1486), der auch die Anzahl der Teiler eines Produkts mehrerer Primzahlen bestimmte, und Ähnliches ausnehmen, vollkommen unbewegt, bis sie mit der Wiedererweckung des Diophant selbst ihre Auferstehung beging. Schon im Jahre 1621 gab Bachet de Méziriac eine griechische Textausgabe des Diophant mit eigenen Zusätzen heraus, welche manches für uns Beachtenswerte enthalten; insbesondere war es Bachet, der noch bestimmter als irgendwer vor

ihm bei Lösung von Aufgaben der unbestimmten Analysis auf ganzzahlige Auflösungen drang und selbst den Nachweis führte, dafs die Gleichung $ax + by = c$ bei teilerfremden a, b stets solche Auflösungen verstatte. (*Problèmes plaisans et delectables, qui se font par les nombres*, 1612). Viel bedeutender aber wurden für die Zahlentheorie die Zusätze, um welche der ausgezeichnete französische Mathematiker Pierre Fermat (geb. 14. März 1601 bei Toulouse, wo er 1631 Parlamentsrat wurde, gest. 12. Jan. 1665 in Castres) sein Exemplar des Diophant vermehrte und mit denen versehen im Jahre 1670 eine neue Textausgabe des Letztern durch den Sohn Fermats besorgt wurde. In diesen Randbemerkungen, aufserdem auch an anderen Stellen, in seinen *opera varia*, in dem von Wallis 1685 herausgegebenen *commercium epistolicum* u. s. w. hat Fermat eine ganze Reihe höchst bemerkenswerter, vor ihm noch unbekannter zahlentheoretischer Sätze teils bewiesen, gröfstenteils freilich nur ausgesprochen. Bezüglich der letztern behauptet er mehrfach, ihre Beweise zu besitzen; ob er darin sich nicht etwa getäuscht haben mag, ist schwierig zu entscheiden, denn einerseits sind einige derselben, wenn sie auch nicht als falsch erkannt wurden, doch noch heute nicht völlig erwiesen, andere, wie die Behauptung, dafs jede Zahl von der Form $2^{2^k} + 1$ eine Primzahl sei, haben sich als unrichtig herausgestellt, andererseits aber hat auch gerade hier Fermat selbst zugestanden, dafs, obwohl er für die Richtigkeit des Satzes einstehen wolle, sein Beweis desselben nicht vollständig sei. Jedenfalls datiert von diesen Fermatschen Sätzen eine neue Epoche der Zahlentheorie, denn gerade der Mangel an Beweisen für jene ist Ursache geworden, die Aufmerksamkeit und die Bemühungen späterer Mathematiker auf sie zu lenken und so in vergleichsweise kurzer Zeit die Wissenschaft der Zahlen zu der stolzen Höhe zu fördern, die sie im vergangenen Jahrhundert erreicht hat.

Überblicken wir die hauptsächlichsten der Fermatschen Sätze, so gehört ein gröfserer Teil derselben, wie aus ihrem Anschlusse an das Werk des Diophant begreiflich ist, der unbestimmten Analysis an. Hierhin zählt die Auflösung der schon von Bhaskara behandelten Gleichung $ax^2 + 1 = y^2$, die gegenwärtig, obwohl sehr unberechtigterweise, als Pellsche Gleichung benannt ist; abgesehen nämlich von Fermats Bemühungen, der sie 1637 Frénicle zur Lösung vorlegte, waren Wallis und Lord Brouncker diejenigen, welche zuerst einen Weg dazu angaben, und das Verdienst John Pells um dieselbe besteht einzig darin, diese letztere Auflösungsmethode einer „*Teutschen Algebra*“ von Rahn, deren englische Übersetzung er veranlafste, hinzugefügt zu haben. Von Fermats Auflösungsart kennen wir leider nicht mehr als ihren allgemeinen Grundgedanken, doch haben wir vielleicht in diesem den Weg zu erblicken, den

Fermat auch sonst zum Beweise seiner Sätze mag eingeschlagen haben; der cyklischen Methode des Bhaskara ganz analog sucht er die Wahrheit einer Behauptung durch eine descente infinie ou indéfinie, d. h. so zu erweisen, dafs, wenn sie für Zahlen einer gewissen Gröfse nicht zuträfe, sie dann auch falsch sein müfste für andere kleinere Zahlenwerte, die dann wieder verkleinert werden könnten u. s. w., bis man zu Zahlenwerten gelangt, für welche die Behauptung im Gegenteile besteht. Neben andern Sätzen der unbestimmten Analysis, teils auf rationale Dreiecke bezüglich, teils von der Art des Satzes, dafs das System der zwei Gleichungen

$$x^2 + y^2 = z^2, \quad x^2 - y^2 = u^2$$

keine ganzzahlige Lösung besitze, ist derjenige besonders berühmt geworden, welcher die Unmöglichkeit der Gleichung $x^n + y^n = z^n$ für ganzzahlige x, y, z behauptet, sobald $n > 2$; denn trotz der Bemühungen der bedeutendsten Mathematiker ist es bisher noch nicht gelungen, diesen Satz in seiner vollen Allgemeinheit zu beweisen; nur für $n = 3$ und 4 konnte Euler, für $n = 5$ Dirichlet ihn bestätigen, und selbst den tiefdringenden Methoden Kummers entzog sich noch immer eine ganze Reihe von Ausnahmswerten des Exponenten n, für welche demnach die Fermatsche Behauptung bis heut unerwiesen blieb. — Eine weitere Kategorie der Fermatschen Sätze trägt reineren zahlentheoretischen Charakter, diejenigen Sätze nämlich, welche die Darstellung von Zahlen in gewissen ausgezeichneten Formen behaupten; zu ihnen gehören Sätze über die Möglichkeit bezw. die Anzahl der Darstellungen einer Primzahl p oder ihrer Potenzen als Summe zweier Quadrate, sowie besonders der schöne Satz, nach welchem jede Zahl als Summe von Polygonalzahlen einer beliebigen Ordnung, als Summe von drei Dreieckszahlen, von vier Quadraten, fünf Pentagonalzahlen u. s. f. darstellbar sei, ein Satz, der später von Cauchy bestimmtere Fassung und in dieser eine, wie mich bedünkt, vollkommen einwandfreie Begründung gefunden hat. Noch ein anderer Satz endlich, der zumeist gemeint wird, wenn von Fermats Satz die Rede ist, eröffnete der Zahlentheorie ein durchaus neues oder doch bisher nur ganz leise gestreiftes Gebiet, die Lehre von den Potenzresten, d. i. von den Zahlen, die als Reste verbleiben können, wenn Quadrat- oder Kubikzahlen oder irgend welche höhere Potenzen durch eine gegebene Zahl geteilt werden; nach jenem Satze läfst insbesondere, wenn die letztere eine Primzahl p ist, die p^{te} Potenz jeder beliebigen Zahl stets denselben Rest, wie diese Zahl selbst; dieser Fermatsche Satz, der einer beträchtlichen Verallgemeinerung fähig ist, hat sich für die Folge als einer der wichtigsten zahlentheoretischen Sätze überhaupt herausgestellt.

Nicht sogleich nun blühte die Saat auf, welche Fermat mit diesen Sätzen ausgestreut hatte, denn andere auch gerade damals entstehende

Disziplinen, die analytische Geometrie, die rationale Mechanik, die Infinitesimal- und die Wahrscheinlichkeitsrechnung, nahmen in erhöhterem Grade Interesse und Bemühungen der Mathematiker jener Zeit in Anspruch. Es bedurfte eines allumfassenden Genius, um auch der Zahlentheorie zu ihrem Rechte zu helfen, und einen solchen brachte das 18. Jahrhundert in Leonhard Euler, jenem grofsen deutsch-schweizerischen Mathematiker hervor, bei welchem gleich staunenswert die Menge seiner Arbeiten und die Vielseitigkeit der Gebiete ist, in denen er geschaffen, wie die Fülle erfinderischer Gedanken, durch welche, was er darin schuf, bedeutend, ja bahnbrechend geworden ist. Auch innerhalb des zahlentheoretischen Gebietes sind seine Forschungen mannigfaltigster Art; abgesehen von anderen betreffenden Arbeiten Eulers in seiner, von Lagrange mit wertvollen Zusätzen versehenen *Algebra*, seiner *introductio in analysin infinitorum* u. s. w., füllen dieselben zwei starke Bände, welche unter dem Titel *Commentationes Arithmeticae collectae*, Petrop. 1849 herausgegeben worden sind. Teilweise sind sie rein arithmetischer Natur und richten sich hier bis auf die Fundamente dieser Wissenschaft, auf Sätze über die Teilbarkeit der Zahlen u. dgl.; unter ihnen tritt die Betrachtung der jetzt meist als Eulersche Funktion bezeichneten Funktion $\varphi(n)$ hervor, welche die Menge der Zahlen bestimmt, die kleiner als n und teilerfremd zu n sind; hierhin gehören auch Eulers eingehende Untersuchungen über vollkommene und über befreundete Zahlen u. a. m. Besonders aber förderte er die reine Zahlentheorie durch seine umfassende und gründliche Untersuchung der Potenzreste, unter ihnen insbesondere der quadratischen Reste, für welche er sogar schon, der Erste von Allen, jenes berühmte Gesetz erkannt hat, welches später das Reciprocitätsgesetz der quadratischen Reste genannt worden ist. Andererseits bewegten sich Eulers Untersuchungen auch weithin im Gebiete der Diophantischen Analysis, in der Auflösung oder Betrachtung der verschiedensten unbestimmten Gleichungen, wie denn schon erwähnt wurde, dafs er die Fermatschen Gleichungen $x^3 + y^3 = z^3$, $x^4 + y^4 = z^4$ als unmöglich bewies; namentlich auch auf die Pellsche Gleichung waren seine Bemühungen gerichtet. Hierbei konzentrierte sich jedoch sein Interesse in bedeutsamer Weise mehr und mehr auf gewisse Formen der untersuchten Ausdrücke, die, aus zwei oder mehr Unbestimmten im zweiten Grade zusammengesetzt, quadratische Formen genannt worden sind, und so wurden die Fragen, welche ursprünglich auf die Auflösung oder Auflösbarkeit gewisser Gleichungen gerichtet waren, jetzt zu solchen nach der Darstellbarkeit bestimmter Zahlen in derartigen Formen, nach ihren möglichen Teilern u. dgl. m., wodurch die unbestimmte Analysis erst eigentlich zahlentheoretischen Charakter erhält.

Auf diesem Wege sind denn noch in demselben Jahrhundert die

französischen Mathematiker Lagrange und Legendre, denen auch sonst die Zahlentheorie manchen bedeutenden Zuwachs verdankt, namentlich dem Letztgenannten in Bezug auf die Theorie der quadratischen Reste, Euler nachgefolgt und haben insbesondere die arithmetische Theorie der quadratischen Formen mit zwei oder drei Unbestimmten sehr wesentlich bereichert und so ihre systematische Entwicklung schon angebahnt.

Nach dem summarischen Überblick, den wir hiermit über die Geschichte der Zahlentheorie vor Gaufs gegeben haben, ist ohne Zweifel zuzugeben, dafs schon vor diesem eine Fülle interessanter, teils grundlegender, teils höherliegender, entwicklungsfähiger Sätze der Zahlentheorie begründet oder vorhanden gewesen ist. Wenn wir gleichwohl diese als eine Wissenschaft erst von Gaufs an datieren, so bewegt uns dazu der Umstand, dafs alles das, was eine Disziplin zur Wissenschaft macht — feste Grundprinzipien, der leitende Faden allgemeiner Methoden und Gesichtspunkte, systematischer Zusammenhang — der Zahlentheorie erst durch die *Disquisitiones Arithmeticae* verliehen worden ist. Dies epochemachende Werk zerfällt in drei grofse Teile. Im ersten derselben, den Sektionen 1 bis 4, giebt Gaufs auf Grund der einfachsten Euclidischen Sätze einen festen systematischen Aufbau dessen, was wir multiplikative Zahlentheorie genannt haben: die Lehre von den elementaren Teilern der Zahlen, den Kongruenzen, d. i. den Eigenschaften der Reste, welche die Zahlen, durch andere Zahlen geteilt, lassen, und den mannigfachen Gesetzen, die sich hierbei herausstellen; insbesondere die Theorie der binomischen Kongruenzen oder der Potenzreste und als einfachstes und prägnantestes Beispiel der letzteren die ausführliche Theorie der quadratischen Reste, namentlich den ersten strengen Beweis für das Reciprocitätsgesetz derselben. Nicht ohne innersten Zusammenhang mit der letztgenannten Theorie und doch für sich ein zweites grofses Gebiet bezeichnend, welches, neben der multiplikativen Zahlentheorie stehend, gewissermafsen sie zur additiven zurückführt, findet im zweiten der genannten Teile der *Disquisitiones*, ihrer 5. Sektion, die Theorie der quadratischen Formen, der Darstellung der Zahlen durch solche, ihres Zusammenhangs unter einander, der wesentlich von einander verschiedenen u. dgl. m. eine ebenfalls methodische und festgefügte systematische Entwicklung, die alles in sich schliefst, was schon vor Gaufs von Euler, Lagrange, Legendre in diesen Fragen geleistet worden war. Der dritte Teil endlich, die 6. und 7. Sektion, besteht aus Anwendungen der entwickelten Lehren, welche teils arithmetischer Natur sind, wie diejenigen zur Bruchzerlegung, zur Primzahlbestimmung u. a., teils die algebraische Auflösung der Kreisteilungsgleichung vermitteln, eine Anwendung der Zahlentheorie, die ebenso berühmt als wichtig geworden ist, ersteres, da sie für das Problem der Kreisteilung einen

seit vielen Jahrhunderten ersten Fortschritt bedeutete, letzteres, weil sie eine ganz neue Auffassung der Theorie der Gleichungen hervorgerufen hat, bei welcher deren algebraische Auflösung unter dem allgemeineren Gesichtspunkte der Verwandtschaft algebraischer Gröſsen erfaſst wird.

Fast alles nun, was seitdem in der Zahlentheorie weiter gefördert ist — und dies ist eine groſsartige Fülle —, darf als ein Ausbau des Grundstocks, welchen Gauſs in den *Disquis. Arithm.* dem stolzen Gebäude dieser Wissenschaft gegeben, als eine Ausbeute der beiden groſsen Gebiete bezeichnet werden, die er derselben erobert hat; in ihrer weiteren Entwicklung beruht und besteht die gesamte seitherige Zahlentheorie. Gauſs selbst schon erweiterte das erste der gedachten Gebiete in folgenreichster Weise durch die Einführung der sogenannten komplexen ganzen Zahlen von der Form $a + b\sqrt{-1}$. Bezüglich dieser Zahlen führte er und in noch weiterem Umfange P. G. Lejeune-Dirichlet, welchem zudem das Verdienst zukommt, die *Disquis. Arithm.* durch geniale Erfassung des Wesens der einzelnen Probleme erheblich vereinfacht und eigentlich erst dem Verständnisse eröffnet zu haben, den Nachweis, daſs sie von ganz analogen Gesetzen beherrscht werden, wie die gewöhnlichen ganzen Zahlen, und so gelang es ihnen, die Theorie der biquadratischen Reste ganz entsprechend und fast ebenso einfach zu gestalten, wie die der quadratischen Reste. Auf dem von ihnen eingeschlagenen Wege folgte zunächst Eisenstein nach, welcher, wenn ϱ eine kubische Einheitswurzel ist, wie $\sqrt{-1}$ eine biquadratische, für die komplexen ganzen Zahlen von der Form $a + b\varrho$ und mittels derselben für die kubischen Reste völlig entsprechende Gesetze nachwies, als die gewöhnlichen ganzen Zahlen bezw. die quadratischen Reste befolgen. Kummer gelang es alsdann, durch eine geniale That, die Einführung gewisser „idealer Zahlen“, das Gleiche auch für die allgemeineren, aus irgend einer Einheitswurzel gebildeten komplexen ganzen Zahlen festzustellen und so auch die Theorie der Potenzreste jeden beliebigen Grades zu begründen. Endlich führten in neuester Zeit Dedekind und Kronecker und einige andere Forscher die Lehre von den allgemeinsten komplexen, den sogenannten algebraischen ganzen Zahlen in analoger Weise durch und mit ihr die multiplikative Zahlentheorie zu ihrer gröſsten Höhe, zu den allgemeinsten Gesichtspunkten, zu vollkommenem Abschlusse.

Aber auch das andere Gebiet, das der zahlentheoretischen Formen, erweiterte und vertiefte sich zusehends. Hatte schon Gauſs neben der Theorie der binären quadratischen Formen und zu deren Vollendung die ternären in Betracht zu ziehen begonnen, so führten neuere Mathematiker, unter denen besonders Hermite, Selling, Stephen Smith und Minkowski zu nennen sind, die Theorie der letzteren und allgemeiner diejenige der quadratischen Formen mit beliebig viel

Unbestimmten weiter aus und vollendeten sie in ihren wesentlichsten Punkten. Andererseits nahm man neben den quadratischen Formen diejenigen höheren Grades in Angriff, Eisenstein z. B. eine gewisse Gattung kubischer Formen mit drei Unbestimmten, welche die ausgezeichnete Eigenschaft haben, in „Linearfaktoren“ zerlegbar zu sein. Letztere Eigenschaft, die auch den binären quadratischen Formen zukommt, hebt aus allen Formen höheren Grades die zahlentheoretisch interessantesten heraus, insofern die Theorie derjenigen Formen, die sie besitzen, im wesentlichen mit der Theorie der algebraischen ganzen Zahlen identisch, nur eine andere Einkleidung derselben ist. Von solcher Erkenntnis aus kommt der Lehre von den binären quadratischen Formen eine ganz singuläre Bedeutung für das System der Zahlentheorie zu. Eine Frage, welche ursprünglich der unbestimmten Analysis angehört, zunächst also, wie die ganze unbestimmte Analysis, des rechten zahlentheoretischen Charakters ermangelt, die Frage nach den ganzzahligen Lösungen der allgemeinen quadratischen Gleichung mit zwei Unbestimmten, gewinnt solchen Charakter, indem sie zur Frage nach der Darstellung ganzer Zahlen in Gestalt binärer quadratischer Formen sich wandelt; diese neue Frage aber, die ihrer Natur nach ein Gegenstand der additiven Zahlentheorie ist, erweist bei genauerer Betrachtung sich der anderen nach der Zerlegung der Zahlen in komplexe, aus einer gewissen Quadratwurzel gebildete ganze Zahlen äquivalent, wird so zu einer Frage der multiplikativen Zahlentheorie und schlingt sich auf solche Weise wie ein gemeinsames Band um alle Teile dieser Wissenschaft.

Eine Lehre aber, deren Gegenstand auch allen übrigen mathematischen Disziplinen unentbehrlich ist, kann sich nicht in so grofsartiger Weise entwickeln, ohne mit den letzteren eine mehr oder weniger innige Verbindung einzugehen, teils auf sie wirkend, teils sich zur eigenen Förderung ihrer bedienend. Das Erstere sahen wir schon bei Gaufs' Bearbeitung der Kreisteilung, das wichtigste Beispiel des letztern geben die analytischen Methoden, durch welche, im Anschlusse an Euler, Dirichlet die Zahlentheorie bereicherte, um Probleme zu lösen von der Art jenes alten Euclidischen, des Nachweises, dafs die Menge der Primzahlen unendlich ist. Auf solche Weise konnten Aufgaben, deren Lösung sich auf anderem Wege nicht hat darbieten wollen — tiefliegende Fragen der Formentheorie, die Untersuchung der mannigfachen Unregelmäfsigkeiten der Zahlenreihe, wie sie in der Verteilung der Primzahlen in derselben oder in dem sprungweisen Charakter der zahlentheoretischen Funktionen zur Erscheinung kommen — entweder erledigt oder doch erfolgreich in Angriff genommen werden.

Auch für die additive Zahlentheorie haben neuerdings dergleichen Methoden sich nutzbringend erwiesen und namentlich in den Arbeiten

englischer Mathematiker, vornehmlich Sylvesters, für die Zerfällung von Zahlen in Summanden der verschiedensten Art vielfache Erkenntnis geliefert. Gleichwohl fehlt es für diesen Abschnitt der Zahlentheorie sowie auch für die Behandlung unbestimmter Gleichungen, welche aufserhalb der Formentheorie stehen, noch sehr, wie an einer geeigneten Grundlage, so auch an allgemeinen Methoden oder Gesichtspunkten, und es wird noch anhaltender Bemühungen der Forscher bedürfen, um hier zu der gleichen Höhe zu dringen, wie die multiplikative Zahlentheorie sie erreicht hat. Der zweite Teil dieses Werkes will den Versuch machen, nach Möglichkeit in die zerstreuten Teile dieser Disziplin, wenn nicht wissenschaftliche Einheit, doch Ordnung und Verbindung zu bringen.

Nach diesen geschichtlichen Bemerkungen, bei denen wir uns vornehmlich auf das grundlegende M. Cantorsche Werk: Vorlesungen über Geschichte der Mathematik, 1. Bd., 2. Aufl. 1894; 2. Bd. 1892; 3. Bd. 1898 gestützt haben, und die wir im weiteren Laufe des Werkes durch litterarische Nachweise vielfältig ergänzen werden, wenden wir uns nunmehr zur systematischen Darstellung der zahlentheoretischen Lehren, die wir darin zu umspannen uns vorgenommen haben. Über die hauptsächlichsten bereits vorhandenen Lehrbücher oder systematischen Bearbeitungen der Zahlentheorie vgl. man die Encyklopädie der mathematischen Wissenschaften I C 1, p. 555/56; zu den dort genannten Werken ist neuestens noch das Kroneckersche Werk, „Vorlesungen über Mathematik II, erster Abschnitt: Vorlesungen über Zahlentheorie, 1. Band, hrsg. von K. Hensel, 1901“ hinzugetreten.

Erstes Kapitel.

Die ganze Zahl und die einfachsten Rechnungsoperationen.

1. Der Begriff der Zahl*) entspringt aus dem Begriffe der Mehrheit d. i. (in gewöhnlichem Sinne) des Inbegriffs verschiedener oder

*) Dieser Begriff hat in neuerer Zeit eine Reihe von mehr oder weniger eingehenden Erörterungen erfahren; wir nennen nur die folgenden Arbeiten:

E. Schröder, *Lehrbuch der Arithmetik und Algebra*, Leipzig 1873; G. Frege, *Grundlagen der Arithmetik*, Jena 1884; H. Schubert, *System der Arithmetik und Algebra*, Potsdam 1885; J. Tannery, *introduction à la théor. des fonct. d'une variable*, Paris 1886; Helmholtz, *Zählen und Messen*, und Kronecker, *über den Zahlbegriff*, in Philosoph. Aufsätze, E. Zeller zu seinem 50jähr. Jubiläum gewidmet, 1887, die letztere Arbeit auch im Journ. f. die r. u. angew. Math. 101, p. 337; R. Dedekind, *was sind und was sollen die Zahlen?*, Braunschweig 1888, 2. Aufl. 1893; G. Peano, *arithmetices principia nova methodo exposita*, Turin 1889; G. Cantor, *Beiträge zur Begründung der transfiniten Mengenlehre*, Math. Ann. 46, p. 481; 1895.

Von ihnen dürfte diejenige von Dedekind vielleicht die beachtenswerteste sein. Insbesondere kommt ihr gegenüber der Darstellung von Kronecker das Verdienst zu, den Charakter eines endlichen Systems im Gegensatze zum unendlichen in einfachster Weise ausgesprochen und die Rolle des Endlichen bei der Begriffsbestimmung der Zahl ins rechte Licht gesetzt zu haben. Während ich hierin mich Dedekinds Vorgange angeschlossen habe, glaubte ich doch in prinzipieller Hinsicht einen andern Standpunkt einnehmen zu müssen. Indem nämlich Dedekind ausgeht vom Begriffe eines „Systems“ von Dingen, der nur aus demjenigen einer „Mehrheit“ von Dingen durch Abstraktion von deren Ordnung gewonnen wird, eliminiert er die Vorstellung einer Folge, die jeder Auffassung unterschiedlicher Dinge zu Grunde liegt und daher natürlicher Weise jenem Begriffe voransteht. Von hier aus gelangt er durch eine langgestreckte Reihe von Definitionen und Folgesätzen, in deren Fassung und Aufbau die ganze Schärfe des Denkens und die grofse Kunst systematischer Entwicklung sich kundgeben, welche auch sonst die Arbeiten des genannten Forschers auszeichnen, zu einem unendlichen Systeme von Elementen, für welches, nachdem man es geordnet, d. h. die „Folge“ je zweier Elemente definiert hat, die gleichen Gesetze sich nachweisen lassen, wie sie für unsere gewöhnlichen Zahlen charakteristisch sind, und in denen wir daher die letzteren wieder zu erkennen haben. Diese Einführung — ich möchte sagen: a posteriori einer Vorstellung, ohne welche meines Erachtens weder der Begriff des „Systems“ noch auch die „Abbildung“ eines solchen erfafst werden kann, erst in die aus jenem gezogenen Folgerungen will mir wenig natürlich und sachgemäfs erscheinen. In meiner Erörterung des Zahlbegriffs, wie sie der Text giebt, habe ich daher die Vorstellung der Folge zur Grundlage des Ganzen genommen.

doch von uns unterschiedener Objekte (der Elemente der Mehrheit), seien diese letzteren intellektueller oder gegenständlicher Art, Gedanken oder Dinge.

Wir unterscheiden aber Objekte, indem wir jedes einzelne derselben durch einen besonderen Akt unsers Bewufstseins erfassen, d. i. sie in unser Denken oder Vorstellen aufnehmen. Die Unterschiedenheit dieser Akte ist für den Begriff der Mehrheit notwendig, sie reicht aber zugleich auch hin, eine solche zu begründen; denn, wenn wir auch von allen besonderen Eigenschaften der Einzeldinge, wie jene Akte sie uns erkennen lassen mögen, abstrahieren, die Dinge eben nur als Einzeldinge in Betracht ziehen, so bleiben dieselben für uns doch immer noch unterschieden durch den besonderen inneren Akt, der sie uns zum Bewufstsein gebracht hat, sodafs auch dasselbe Objekt, wiederholt gedacht oder vorgestellt, einen Inbegriff unterschiedener Objekte, eine Mehrheit hervorbringt. Aber verschiedene Akte unsers Bewufstseins bilden stets eine Folge, und nur in dieser bestimmten Folge vermögen wir die unterschiedenen Einzeldinge zur Mehrheit zusammenzufassen; die Mehrheit stellen wir demnach genauer als „Inbegriff einer bestimmten Folge von Objekten“ fest.

Geschieht nun, wie gesagt, die Unterscheidung eines Objektes von einem andern dadurch, dafs wir jedes derselben mit einem besonderen Akte unsers Bewufstseins erfassen, so ist doch behufs der Unterscheidung gleichgiltig, welches der Elemente zuerst, welches zuletzt erfafst wird; die Folge der Akte läfst sich dabei vertauschen. Durch solche Vertauschung gelangt man zu einer anderen Anordnung derselben Objekte und durch die neue Zusammenfassung der letzteren zu einer Mehrheit, die aus denselben Elementen, wie die frühere, aber in anderer Anordnung besteht. Indem man dann bei diesen Mehrheiten von der Anordnung ihrer Elemente abstrahiert, entsteht der neue Begriff der Gesamtheit oder des Systemes von Elementen oder Objekten, welches für eine Mehrheit M durch $\overline{M}$ bezeichnet werden soll.

Eine Mehrheit heifse ein Teil einer anderen, wenn die unterschiedenen Elemente der ersteren zugleich unterschiedene Elemente der letzteren sind, ein echter Teil, wenn hierbei nicht die Gesamtheit der letzteren auch diejenige der ersteren ist; ist im Gegenteil dieses der Fall, so sind die Mehrheiten entweder identisch oder nur durch die Anordnung ihrer Elemente verschieden.

Wird bei einer Mehrheit M nicht nur von der Anordnung ihrer Elemente abgesehen und so der Begriff des Systems $\overline{M}$ gewonnen, sondern abstrahiert man zudem auch von jeder besonderen Beschaffenheit der Elemente, indem man diese nur als Einzelobjekte (als „Einsen“) in Betracht nimmt, so erhält man den Begriff

der Vielheit (Mächtigkeit), welche der Mehrheit M entspricht und welche durch $\overline{\overline{M}}$ bezeichnet werden möge, „das intellektuelle Abbild, die Projektion der Menge M in unserm Geiste" (G. Cantor).

2. In den aufeinanderfolgenden Akten unsers Bewufstseins tragen wir in uns eine spontan sich bildende Mehrheit, auf die jede andere Mehrheit, die wir erfassen, bezogen wird, indem den successiven Elementen der ersteren die einzelnen Elemente der letzteren sich zuordnen. Diesen inneren Vorgang zu versinnlichen, hat der menschliche Geist seit den ältesten Zeiten Methoden erdacht, um entsprechend jener spontan sich bildenden Mehrheit eine Reihe von Zeichen zu bilden, die deren Stelle vertritt, und so jene Beziehung einer anderen Mehrheit zur letzteren, d. i. die Stelle, welche jedem Elemente der Mehrheit in der Folge der Denk- oder Vorstellungsakte zukommt, durch Beilegung des entsprechenden Zeichens (als Index oder Stellenzeiger) zu sinnfälligem Ausdrucke zu bringen. Diese Zeichen sind die Zahlen (als Ordinalzahlen), in unserer abendländischen Schreibweise also die Zeichen:

$$1, 2, 3, 4, 5, 6, 7, \ldots \tag{O}$$

In der Regel, nach welcher diese Zeichen successive gebildet werden, beruht sowohl die Möglichkeit, ihre Reihe „unbegrenzt" fortzusetzen, als auch die Möglichkeit, sie bis zu einem beliebig fernen Gliede n hin, d. h. die Zahlen der „begrenzten" Reihe $1, 2, 3, \ldots n$ sämtlich zu bilden, diese Reihe zu durchlaufen, bis zu n zu gelangen.

Werden nun den Zahlen der Reihe nach die Elemente einer Mehrheit zugeordnet, so sagt man: diese Elemente werden markiert oder gezählt. Hiernach wird eine Mehrheit als gegeben anzusehen sein, wenn die einzelnen der Zahlenreihe zugezählten Objekte, soweit es deren giebt, bestimmt sind, sei es, dafs wir sie sämtlich einzeln aufzufassen vermögen, wie etwa die Finger einer Hand, sei es, dafs wir nur nach einem bestimmten Gesetze oder einer Regel sie successive bilden oder aufstellen können, wie z. B. die Reihe der Zahlen selbst.

3. Seien solcherweise die Mehrheiten M_1, M_2 gegeben. Durch die gemeinsame Zuordnung ihrer Elemente zur Zahlenreihe wird eine Beziehung ihrer Elemente zu einander vermittelt derart, dafs die Elemente der einen Mehrheit, welche unterschiedenen Elementen der anderen zugeordnet sind, auch unterschieden sind. Falls hierbei jedem Elemente von M_1 ein Element von M_2 zugeordnet ist, soll so M_1 eindeutig auf M_2 bezogen (nach Dedekind: in M_2 abgebildet) heifsen; und wenn dadurch auch umgekehrt M_2 eindeutig auf M_1 bezogen ist, so sollen die Mehrheiten M_1, M_2 einander ähnlich (Kronecker und Cantor: äquivalent) genannt werden.

Ist M_1 eindeutig auf M_2 bezogen, so wird hiermit offenbar auch jeder Teil von M_1 eindeutig auf einen gewissen Teil von M_2 bezogen sein.

Satz I. Sind demnach M_1, M_2 ähnliche Mehrheiten, so ist auch jeder Teil der einen von ihnen einem Teile der andern ähnlich.

Satz II. Sind M_1, M_2 ein- und derselben Mehrheit M ähnlich, so sind sie es ersichtlich auch unter einander.

Satz III. Mehrheiten M_1, M_2, die sich nur durch die Anordnung ihrer Elemente von einander unterscheiden, sind ähnlich, denn sie sind beide der Vielheit $\overline{\overline{M}}$, die ihnen gemeinsam ist, und daher auch die eine der anderen in eindeutiger Weise zugeordnet.

Satz IV. Die Ähnlichkeit der Mehrheiten M_1, M_2 ist gleichbedeutend mit der Identität der entsprechenden Vielheiten $\overline{\overline{M}}_1$, $\overline{\overline{M}}_2$; mit andern Worten: aus der Ähnlichkeit von M_1, M_2 folgt $\overline{\overline{M}}_1 = \overline{\overline{M}}_2$ und umgekehrt. In der That bleibt nach der Definition der Vielheit $\overline{\overline{M}}_1$ ungeändert, wie auch die besondere Beschaffenheit der Elemente der Menge M_1 verändert wird, z. B. also, falls M_1, M_2 ähnlich sind, wenn jedes dieser Elemente durch das ihm zugeordnete der Menge M_2 ersetzt wird; da so die Mehrheit M_1 sich in die Mehrheit M_2 verwandelt, deren Vielheit $\overline{\overline{M}}_2$ ist, folgt in der gemachten Voraussetzung $\overline{\overline{M}}_1 = \overline{\overline{M}}_2$. Ist aber die Vielheit $\overline{\overline{M}}_1$ und die Vielheit $\overline{\overline{M}}_2$ ein- und dieselbe, so sind die Mehrheiten M_1, M_2, weil sie in eindeutiger Weise dieser selben Vielheit zugeordnet sind, es auch unter einander, w. z. b. w.

4. Nun sind für eine Mehrheit M nur folgende Fälle denkbar: entweder giebt es einen echten Teil $\mathfrak{M}$ von M, welchem M ähnlich ist, oder es giebt einen solchen nicht. Im erstern Falle heiſse M eine unendliche, im letztern eine endliche Mehrheit (Dedekind).

Satz I. Ähnliche Mehrheiten M_1, M_2 sind beide zugleich endlich oder zugleich unendlich. Denn, wäre eine derselben, z. B. M_1 unendlich und $\mathfrak{M}_1$ ein echter Teil von M_1, welchem M_1 ähnlich wäre, so gäbe es auch einen mit $\mathfrak{M}_1$ ähnlichen Teil $\mathfrak{M}_2$ von M_2 (Nr. 3, Satz I), welchem (nach Nr. 3, Satz II) M_1 und folglich (desgl.) auch M_2 ähnlich sein würde. Dieser Teil $\mathfrak{M}_2$ von M_2 kann aber nur ein echter Teil und deshalb muſs M_2 unendlich sein, denn, da $\mathfrak{M}_1$ diejenigen Elemente von M_1 enthält, welche den in $\mathfrak{M}_2$ enthaltenen Elementen von M_2 entsprechen, so würde, wenn $\mathfrak{M}_2$ jedes Element von M_2 enthielte, in $\mathfrak{M}_1$ jedes Element von M_1 enthalten sein, das einem Elemente von M_2 entspricht, d. h. $\mathfrak{M}_1$ enthielte alle Elemente von M_1, gegen die Voraussetzung.

Satz II. Jeder Teil $\mathfrak{M}$ einer endlichen Mehrheit M ist endlich. Dies leuchtet, wenn $\mathfrak{M}$ die Mehrheit M selbst oder nur durch die Anordnung der Elemente von ihr verschieden ist, aus dem vorigen Satze ein, denn alsdann sind $\mathfrak{M}$ und M ähnlich. Ist aber $\mathfrak{M}$ ein echter Teil von M, so sei $\mathfrak{N}$ die nach Ausscheidung der in ihm enthaltenen Elemente aus M verbleibende Mehrheit. Wäre nun $\mathfrak{M}$ eine unendliche Mehrheit, gäbe es also einen echten Teil $\mathfrak{M}'$ von $\mathfrak{M}$, dem $\mathfrak{M}$ ähnlich wäre, so wäre die aus den Elementen von $\mathfrak{M}'$ und $\mathfrak{N}$ gebildete Mehrheit ein echter Teil der aus $\mathfrak{M}$ und $\mathfrak{N}$ gebildeten Mehrheit, die sich von M nur durch verschiedene Anordnung der Elemente unterscheiden kann; diese würde aber, da $\mathfrak{M}$ mit $\mathfrak{M}'$ und $\mathfrak{N}$ mit sich selbst ähnlich ist, jenem Teile ähnlich und folglich unendlich sein, während sie doch, da M als endlich vorausgesetzt ist, dem anfangs Gesagten zufolge gleichfalls endlich sein mufs.

5. Die Zahlenreihe (O) ist eine unendliche Mehrheit, denn die „geraden“ Zahlen 2, 4, 6, 8, ... bilden einen offenbar echten Teil ihrer Gesamtheit, dessen Elementen die sämtlichen Zahlen (O) eindeutig zugeordnet werden können, und umgekehrt.

Begrenzte Teile der Zahlenreihe, welche aus, von 1 an aufeinanderfolgenden Zahlen $1, 2, 3, \ldots n$ bestehen, sollen Abschnitte derselben heifsen, in Zeichen:

$$|1, 2, 3, \ldots n|.$$

Jeder dieser successiven Abschnitte:

$$\text{(A)} \qquad |1|, \ |1, 2|, \ |1, 2, 3|, \ |1, 2, 3, 4|, \ldots$$

ist ersichtlich ein echter Teil des nächstfolgenden und daher auch der späteren Abschnitte.

Jeder Abschnitt ist eine endliche Mehrheit. Wir nehmen an, dies sei bewiesen für den Abschnitt $N = |1, 2, 3, \ldots n|$, und zeigen es dann auch für den folgenden Abschnitt $M = |1, 2, 3, \ldots n, n'|$, wo n' die auf n folgende Zahl bezeichne; da es offenbar für den ersten Abschnitt $|1|$, der überhaupt keinen echten Teil hat, richtig ist, gilt es dann allgemein. — Gesetzt nun, der Abschnitt M sei einem echten Teile $\mathfrak{M}$ seiner selbst ähnlich, so sind nur folgende Fälle denkbar: entweder wird bei der ähnlichen Beziehung des Abschnittes auf seinen Teil die Zahl n' auf sich selbst bezogen oder auf eine Zahl m der Reihe $1, 2, 3, \ldots n$. Im erstern Falle bestünde $\mathfrak{M}$ aus n' und einem echten Teile der letzteren Reihe und der Abschnitt N würde somit einem echten Teile seiner selbst ähnlich sein, während doch angenommen worden ist, dafs er endlich sei; dieser Fall ist also unzulässig. Im anderen Falle folgert man dasselbe in gleicher Weise, falls n' in $\mathfrak{M}$ nicht auftritt. Ist aber n' darin vorhanden, indem eine Zahl p der Reihe $1, 2, 3, \ldots n$ bei der ähnlichen Beziehung des Abschnittes M auf seinen Teil auf n' bezogen wird, so würde derjenige

Teil $\mathfrak{N}$ des Abschnittes N, in welchem p fehlt, dem Teile $\mathfrak{M}'$ von $\mathfrak{M}$ ähnlich sein, in welchem n' und m unterdrückt sind und welcher somit jedenfalls ein echter Teil von $\mathfrak{N}$ sein würde, wenn die Zahl p (was für $p = m$ der Fall wäre) in $\mathfrak{M}'$ nicht auftritt; andernfalls dürfte man in $\mathfrak{M}'$ diese Zahl, ohne die ähnliche Beziehung der Mehrheiten $\mathfrak{N}$ und $\mathfrak{M}'$ zu einander zu stören, durch die Zahl m ersetzen und fände so wieder $\mathfrak{N}$ einem echten Teile seiner selbst ähnlich, denn, wenn $\mathfrak{M}'$ das Element p enthält, kann es nicht zugleich alle Elemente von $\mathfrak{N}$ nach Ausschlufs von m, also, wenn p durch m ersetzt wird, nicht alle Elemente von $\mathfrak{N}$ enthalten, ohne dafs $\mathfrak{M}$ sämtliche Elemente von M enthielte; $\mathfrak{N}$ und (nach Nr. 4, Satz II) folglich auch N wären mithin unendlich, gegen die Voraussetzung, und somit erweist sich auch der letzte, allein noch übrige Fall als unzulässig.

6. Nachdem dies festgestellt ist, bezeichnen wir die nach voriger Nummer endlichen Vielheiten, welche den successiven Abschnitten (A) zukommen, kurz wieder durch die ihnen charakteristischen Zahlen

(K) $$1, 2, 3, 4, 5, 6, 7, \ldots$$

oder nennen sie die Einheit, Zweiheit, Dreiheit, u.s.w. Die Zeichen (O), welche wir zunächst — als Ordinalzahlen — zur Bezeichnung der Folge eingeführt haben, erhalten so eine abweichende, neue Bedeutung als Zeichen für gewisse Vielheiten, eine Bedeutung, in welcher sie nun Kardinalzahlen oder ganze Zahlen genannt werden.

Satz I. Die Vielheiten, welche durch verschiedene Zahlen bezeichnet werden, d. i. verschiedenen Abschnitten entsprechen, können nicht identisch sein; in der That würden sonst (nach Nr. 3, Satz IV) diese Abschnitte einander ähnlich sein; da aber der frühere von ihnen ein echter Teil des späteren ist, müfste der letztere unendlich sein, was nicht zutrifft.

Satz II. Jede endliche Mehrheit ist einem bestimmten Abschnitte ähnlich. Denn durch die Zuordnung ihrer Elemente zu den aufeinanderfolgenden Zahlen ist eine eindeutige Beziehung der Mehrheit zur Zahlenreihe (O) gegeben, durch deren Umkehrung aber nicht zugleich auch die Zahlenreihe eindeutig auf M bezogen werden kann, denn sonst wäre die unendliche Zahlenreihe der endlichen Mehrheit ähnlich, gegen Nr. 4, Satz I. Demnach wird es Zahlen geben, denen kein Element von M zugehört; eine von ihnen sei n' und die nächst vorhergehende Zahl heifse n. Aus der Zuordnung der Elemente von M zur Reihe aufeinanderfolgender Zahlen ergiebt sich unmittelbar, dafs dann auch keiner der auf n' folgenden Zahlen ein Element von M zugehört, die Elemente dieser Mehrheit vielmehr nur von 1 an aufeinanderfolgenden Zahlen der Reihe $1, 2, 3, \ldots n$ und somit sie und die Zahlen einer der Folgen

$$1;\ 1, 2;\ 1, 2, 3;\ \ldots;\ 1, 2, 3, \ldots n,$$

deren gesamte Reihe zugleich mit der Reihe $1, 2, 3, \ldots n$ durchlaufen werden kann, sich zugeordnet sind. Mithin ist die Mehrheit M selbst einem gewissen Abschnitte $|1, 2, 3, \ldots m|$, wo m eine der Zahlen $1, 2, 3, \ldots n$ bedeutet, und, da verschiedene Abschnitte, wie kurz vorher bemerkt, nicht einander und deshalb auch einer gemeinsamen Mehrheit nicht ähnlich sein können, auch nur diesem Abschnitte ähnlich.

Hiernach stimmt die Dedekindsche Fassung des Endlichen im Grunde mit der gewöhnlichen, welche das Endliche mit dem Begrenzten identifiziert, überein. Nennt man nämlich eine Mehrheit endlich, wenn sie durch eine begrenzte Reihe von Zahlen $1, 2, 3, \ldots m$ abgezählt werden kann, oder dem Abschnitte $|1, 2, 3, \ldots m|$ ähnlich ist, so ist sie auch im Dedekindschen Sinne endlich (nach Nr. 5 und Nr. 4, Satz I); umgekehrt ist eine in diesem Sinne endliche Mehrheit es auch im gewöhnlichen Sinne, weil sie, wie soeben bewiesen, einem Abschnitte ähnlich ist.

Die durch den vorigen Satz bestimmte ganze Zahl m — die Kardinalzahl nämlich, welche die dem Abschnitte $|1, 2, 3, \ldots m|$ zugehörige Vielheit ausdrückt — heifst die Anzahl der Elemente der endlichen Mehrheit M.

Satz III. Offenbar ist die Anzahl der Elemente für endliche Mehrheiten, die einander ähnlich sind, dieselbe; und umgekehrt sind zwei endliche Mehrheiten mit gleicher Elementen-Anzahl, weil ein- und demselben Abschnitte ähnlich, es auch untereinander.

Die Anzahl der Elemente des Abschnittes $|1, 2, 3, \ldots m|$ ist gleich m.

Die Elemente einer endlichen Mehrheit M, deren Anzahl m ist, dürfen vermöge ihrer eindeutigen Beziehung zum Abschnitte $|1, 2, 3, \ldots m|$ durch $E_1, E_2, \ldots E_m$ angedeutet werden.

Wir nennen nun in der Reihe (K) der ganzen Zahlen eine jede gröfser als jede der voraufgehenden, kleiner als jede der ihr folgenden Zahlen. Mit dieser Gröfsenordnung für die 'ganzen Zahlen ist auch für die Anzahl der Elemente endlicher Mehrheiten die Gröfsenordnung bestimmt. Sind nämlich M, M' solche Mehrheiten und m, m' die ihnen resp. entsprechenden Anzahlen, so werden entweder M, M' einander ähnlich sein und dann ist die Anzahl m dieselbe, wie die Anzahl m'; im entgegengesetzten Falle sind M, M' verschiedenen Abschnitten ähnlich, also (vgl. Satz I) sind m, m' verschiedene Zahlen der Reihe (K) und folglich mufs dann entweder m gröfser oder kleiner als m' sein. In Zeichen setzt man je nach diesen Fällen, von denen ein einziger notwendig stattfindet,

$$m = m';\quad m > m';\quad m < m'.$$

7. Unter *einem Stück der Zahlenreihe* (O) verstehen wir eine endliche, aus aufeinanderfolgenden Zahlen gebildete Mehrheit. Ist $|1, 2, 3, \ldots \nu|$ der Abschnitt der Zahlenreihe, welchem sie ähnlich ist, so kann sie durch $|n_1, n_2, \ldots n_\nu|$ bezeichnet werden.

Seien nun M, M zwei endliche Mehrheiten mit durchweg von einander unterschiedenen Elementen, indem nicht nur diejenigen von M und diejenigen von M für sich, sondern auch die erstern von den letztern unterschieden werden, und seien n, ν die ihnen entsprechenden Anzahlen. Dann ist M ähnlich dem Abschnitte $|1, 2, 3, \ldots n|$, M dem Abschnitte $|1, 2, 3, \ldots \nu|$ also auch dem Stücke

$$|n_1, n_2, \ldots n_\nu|,$$

wobei für n_1 die auf n folgende Zahl gewählt werden darf. Die gesamte, aus den Elementen von M und M aneinandergefügte Mehrheit wird demzufolge dem Abschnitte

$$|1, 2, 3, \ldots n, \; n_1, n_2, \ldots n_\nu|$$

ähnlich, mithin eine endliche Mehrheit sein. Die Anzahl ihrer Elemente, welche die gleiche bleibt, wenn M und M durch bezw. ähnliche Mehrheiten M' und M' ersetzt werden, da die aus den letzteren aneinandergefügte Mehrheit der zuvor gebildeten ersichtlich auch ähnlich ist, heifst *die Summe von* n, ν, in Zeichen:

$$n + \nu,$$

die Zahlen n, ν heifsen *Summanden*, und die Operation, die Summe zu bilden, *die Addition von* ν *zu* n. Da bei der Bestimmung der Vielheit also auch der Anzahl von jeder bestimmten Anordnung der Elemente abgesehen wird, bleibt diese Summe ungeändert, in welcher Folge auch die Elemente von M und M zusammengefafst werden, wenn z. B. also, statt M an M zu fügen, umgekehrt die Elemente von M an diejenigen von M gefügt werden; man findet hiernach die Beziehung

$$n + \nu = \nu + n,$$

d. h. *die Addition ist eine kommutative Operation.* Ebenso einfach erkennt man durch Hinzunahme noch einer dritten Mehrheit $\mathfrak{M}$ mit der Elementen-Anzahl $\mathfrak{n}$, dafs *die Addition auch eine associative Operation*, nämlich

$$(n + \nu) + \mathfrak{n} = n + (\nu + \mathfrak{n})$$

ist. Wie die Summe zweier Zahlen, so läfst sich hiernach auch die Summe von drei, dann von vier, fünf Zahlen u. s. w., d. i. die Summe jeder endlichen Anzahl von Zahlen in völlig bestimmter Weise bilden.

Da der Abschnitt $|1, 2, 3, \ldots n, n'|$ sich aus dem Abschnitte $|1, 2, 3, \ldots n|$ und der Zahl n' zusammensetzt, Mehrheiten mit der Anzahl n, 1 resp., während n' die Anzahl des gesamten Abschnittes

bezeichnet, so findet sich nach dem Vorigen $n' = n + 1$, d. h. die auf n folgende ganze Zahl entsteht durch Addition der Einheit zur Zahl n.

Da $n' > n$, so ist $n + 1 > n$ und man sieht allgemeiner ein, dafs die Summe $n + \nu > n$ ist. Ist umgekehrt $m > n$, so giebt es eine (und nur eine) bestimmte ganze Zahl ν so beschaffen, dafs $n + \nu = m$ ist. Denn, heifsen im Abschnitte $|1, 2, 3, \ldots m|$, von welchem der Abschnitt $|1, 2, 3, \ldots n|$ ein echter Teil ist, die auf n folgenden Zahlen $p, q, \ldots m$, so ist er zusammengefügt aus den Mehrheiten

$$|1, 2, 3, \ldots n| \quad \text{und} \quad |p, q, \ldots m|,$$

deren letzte, als Teil eines endlichen Abschnittes, nach Nr. 4, Satz II endlich ist und demnach eine bestimmte Anzahl ν von Elementen besitzt; hieraus findet sich aber $m = n + \nu$. Gäbe es nun noch eine von ν verschiedene ganze Zahl $\mathfrak{n}$, für welche ebenfalls $m = n + \mathfrak{n}$ wäre, so würde m die Anzahl der aus den Abschnitten $|1, 2, 3, \ldots n|$ und $|1, 2, 3, \ldots \mathfrak{n}|$ zusammengefügten Mehrheit

$$1, 2, 3, \ldots n, \; 1, 2, 3, \ldots \mathfrak{n},$$

welcher daher (nach Nr. 6, Satz III) der Abschnitt

$$|1, 2, 3, \ldots n, \; p, q, \ldots m|$$

ähnlich sein müfste; mithin wäre die Mehrheit $p, q, \ldots m$ dem Abschnitte $|1, 2, 3 \ldots \mathfrak{n}|$ ähnlich und daher $\mathfrak{n}$ gleich der ihr zugehörigen Anzahl ν, gegen die Voraussetzung.

Aus der Gleichheit $n + \nu = n + \mathfrak{n}$ erschliefst man mithin stets die andere: $\nu = \mathfrak{n}$, denn sonst gäbe es für die Zahl $m = n + \nu > n$ noch eine zweite, davon verschiedene Darstellung $m = n + \mathfrak{n}$.

Die so bestimmte ganze Zahl ν wird die Differenz oder der Unterschied von m und n genannt, in Zeichen:

$$\nu = m - n,$$

ihre Bildung heifst die Subtraktion der Zahl n (des Subtrahenden) von der (gröfseren) Zahl m (dem Minuenden).

Da $n + \nu = \nu + n = m$ ist, folgert man

$$n + (m - n) = (m - n) + n = m.$$

Ist m die auf n folgende Zahl, also $m = n + 1$, so ergiebt sich $n = m - 1$, d. h. die vor m voraufgehende Zahl entsteht aus m durch Subtraktion oder Wegnahme der Einheit; allgemeiner erkennt man, dafs die Differenz ν aus m durch successive Wegnahme von n Einheiten entsteht.

In jeder endlichen Menge von Zahlen $p, q, r, s, \ldots$, z. B. wenn diese Zahlen Elemente aus dem Abschnitte $|1, 2, 3, \ldots n|$ sind,

ist *eine die kleinste* (genauer: gleich oder kleiner als jede der übrigen) *und eine die gröfste* (genauer: gleich oder gröfser als jede der übrigen). Dies leuchtet unmittelbar ein für jede Menge zweier Zahlen p, q, wobei, falls etwa $p = q$ wäre, die kleinste Zahl mit der gröfsten übereinstimmen würde. Nehmen wir an, es gelte für jede Menge von n Zahlen, so gilt es auch für jede Menge von $n + 1$ Zahlen, also nach bekannter Schlufsweise allgemein. In der That sei $p, q, r, s, \ldots$ eine Menge von $n + 1$ Zahlen, so bilden dem Voraufgehenden zufolge $q, r, s, \ldots$ eine solche von n Zahlen; ist nun k die kleinste, g die gröfste Zahl dieser Menge, so sind nur folgende Fälle möglich: entweder ist $p \leqq k$, dann ist p die kleinste, g die gröfste Zahl der Menge $p, q, r, s, \ldots$; oder es ist $p > k$ aber zugleich $p \leqq g$, dann bilden k, g, oder endlich, wenn $p > g$ wäre, so bilden k, p die kleinste und die gröfste Zahl der Menge $p, q, r, s, \ldots$, w. z. b. w.

8. Denkt man eine endliche Mehrheit M, deren Bestandteile n endliche Mehrheiten von gleicher Anzahl ν der Elemente sind, so ist die Mehrheit M dem Vorigen zufolge auch in Bezug auf die Elemente jener n Mehrheiten endlich und die gesamte Anzahl dieser ihrer Elemente *ist die Summe von n gleichen Summanden ν. Eine solche Summe heifst das Produkt aus n und ν und wird mit $n.\nu$ oder $n\nu$ bezeichnet*, die Zahlen n, ν *als die Faktoren* desselben, und die Operation, das Produkt zu bilden, *als die Multiplikation von ν mit n.* Nennt man die n Mehrheiten $M_1, M_2, \ldots M_n$ und die Elemente von M_i, wo i jede der Zahlen $1, 2, 3, \ldots n$ bedeutet, $E_1^i, E_2^i, \ldots E_\nu^i$, so erhält man die sämtlichen unterschiedenen Elemente von M aus dem Zeichen E_k^i, wenn man dem Index i jeden der Werte $1, 2, 3, \ldots n$, dem Index k jeden der Werte $1, 2, 3, \ldots \nu$ beilegt. Hierbei bilden aber die Zeichen $E_k^1, E_k^2, \ldots E_k^n$, welche ein- und demselben Werthe von k entsprechen, eine endliche Mehrheit $\mathfrak{M}_k$ von n Elementen, und die aus den ν Mehrheiten $\mathfrak{M}_1, \mathfrak{M}_2, \ldots \mathfrak{M}_\nu$ aneinandergefügte Mehrheit besteht aus genau denselben, nur anders geordneten unterschiedenen Elementen E_k^i, wie M, mit deren Anzahl $n\nu$ daher die ihr zukommende Anzahl, welche offenbar νn ist, übereinstimmen mufs. So findet sich die Beziehung

$$n\nu = \nu n,$$

d. h. *die Multiplikation ist eine kommutative Operation.* Auf ähnliche Weise erkennt man, indem man noch eine dritte Mehrheit mit der Anzahl $\mathfrak{n}$ hinzuzieht, dafs *die Multiplikation auch associativ ist*, d. h. dafs die Beziehung

$$(n\nu)\mathfrak{n} = n(\nu\mathfrak{n})$$

stattfindet. Demnach ist das Produkt jeder endlichen Anzahl von Zahlen in völlig bestimmter Weise zu bilden. Der Multiplikation

kommt aber noch eine dritte Eigenschaft, die der Distribuitivität, zu, welche sich in der Formel

$$(n+\nu)\,\mathfrak{n} = n\mathfrak{n} + \nu\mathfrak{n} = \mathfrak{n}n + \mathfrak{n}\nu = \mathfrak{n}\,(n+\nu)$$

ausspricht und sich durch analoge Betrachtungen herleiten läſst.

Aus der Gleicheit $n\nu = n\mathfrak{n}$ folgt stets die andere: $\nu = \mathfrak{n}$. Denn andernfalls wäre eine der Zahlen ν, $\mathfrak{n}$ gröſser als die andere, etwa $\nu > \mathfrak{n}$, es gäbe mithin eine ganze Zahl z so beschaffen, daſs $\nu = \mathfrak{n} + z$ ist, und man erschlösse aus der vorausgesetzten Gleichheit diese neue:

$$n\mathfrak{n} + nz = n\mathfrak{n},$$

welche unmöglich ist, da die Summe zur Linken im Gegenteil gröſser ist als $n\mathfrak{n}$.

Ein Produkt aus ν gleichen Faktoren n heiſst eine Potenz und wird mit n^ν, n als ihre Basis, ν als ihr Exponent bezeichnet. Da die Multiplikation associativ ist, besteht folgende Beziehung:

$$n^\nu \,.\, n^{\mathfrak{n}} = n^{\nu+\mathfrak{n}} = n^{\mathfrak{n}+\nu} = n^{\mathfrak{n}} \,.\, n^\nu.$$

Ferner ist

$$n^\nu \,.\, \mathfrak{n}^\nu = (n\mathfrak{n})^\nu.$$

Zum Beweise nehme man an, diese Beziehung sei richtig, und erweise sie dann auch für den nächst gröſseren Exponenten $\nu + 1$; da sie für $\nu = 1$ der Definition der Potenz und des Produktes zufolge besteht, so besteht sie dann allgemein. Nun folgt aus ihr durch Hinzufügung des Faktors $n\mathfrak{n}$

$$n^\nu\mathfrak{n}^\nu \,.\, n\mathfrak{n} = (n\mathfrak{n})^\nu \,.\, n\mathfrak{n} = (n\mathfrak{n})^{\nu+1},$$

während aus der Kommutativität der Multiplikation die linke Seite sich mit $n^\nu n \,.\, \mathfrak{n}^\nu\mathfrak{n}$, d. i. mit $n^{\nu+1} \,.\, \mathfrak{n}^{\nu+1}$ identisch ergiebt, w. z. b. w.

9. Die Addition und die Multiplikation zweier Zahlen kann stets ausgeführt werden, führt nämlich immer zu einer bestimmten ganzen Zahl, welche die Summe oder das Produkt jener beiden ist. Dagegen ist der Begriff der Differenz $m - n$ von vornherein durch die Voraussetzung beschränkt, daſs die erste der Zahlen m, n gröſser als die andere sei, hätte also im entgegengesetzten Falle keinen Sinn. Gleichwohl kann man auch in ihm der Differenz durch folgende Betrachtung einen Sinn unterlegen. Sei M eine Zahl, welche gröſser ist als jede der beiden Zahlen m, n, sodaſs man, unter z eine ganze Zahl verstehend, $M = z + m$ setzen darf. Dann findet sich, falls $m > n$ ist, ohne Mühe die Beziehung

$$(z+m) - n = z + (m-n); \tag{1}$$

denn, setzt man $m - n = \nu$ also $m = \nu + n$, so ist $z + m = (z+\nu) + n$, mithin

$$(z+m) - n = z + \nu = z + (m-n).$$

Falls dagegen $m < n$ also etwa $n = m + \mu$ ist, darf man

$$(z + m) - n = (z + m) - (\mu + m)$$

einer ganzen Zahl δ gleich, mithin $z + m = \mu + m + \delta$, $z = \mu + \delta$ d. i.

$$\delta = z - \mu$$

setzen, eine Formel, welcher nach der Bedeutung der Zeichen μ, δ die Form

$$(z + m) - n = z - (n - m) \tag{2}$$

gegeben werden kann. In demselben Falle hat nun zwar das Zeichen $m - n$ von vornherein keinen Sinn; definiert man es aber in diesem Falle durch die (im entgegengesetzten Falle aus dem Begriffe der Differenz $m - n$ folgende) Beziehung (1), so ergiebt die Vergleichung derselben mit der Beziehung (2) die Formel

$$z + (m - n) = z - (n - m)$$

oder noch einfacher die Formel

$$+ (m - n) = - (n - m), \tag{3}$$

falls $m < n$.

Die in diesem Falle giltige Formel (2) ist von vornherein ohne Bedeutung, wenn $m > n$ ist, dann aber besteht die Beziehung (1). Nimmt man also alsdann die Formel (2) zur Definition des Zeichens $-(n - m)$, so zeigt ihre Vergleichung mit jener, dafs

$$z - (n - m) = z + (m - n)$$

oder

$$- (n - m) = + (m - n)$$

ist, falls $m > n$, oder, bei Vertauschung der Zeichen m, n, dafs

$$- (m - n) = + (n - m) \tag{4}$$

ist, falls $m < n$.

Durch die definierenden Formeln (1) und (2) ist dem Differenzzeichen $m - n$ auch in dem Falle, wo der Minuendus kleiner ist als der Subtrahendus, eine bestimmte, zunächst rein operative Bedeutung beigelegt der Art, dafs die Addition einer solchen Differenz mit der Wegnahme, die Subtraktion derselben mit der Hinzufügung der ganzen Zahl $n - m$ gleichbedeutend ist. Nennt man aber jede im Lauf einer Rechnung additiv auftretende Zahl eine positive, jede subtraktiv auftretende Zahl eine negative, so darf man jetzt die Differenz $m - n$, falls $m < n$ ist, auch losgelöst von der Rechnung, in der sie auftritt, als eine Zahl ansprechen, indem man kurz so sich ausdrückt:

Ist $m < n$, so ist die Differenz $m - n$ die negative Zahl $-(n - m)$, und diese negative Zahl addieren bezw. subtra-

hieren heifst ihren absoluten oder Zahlenwert $n - m$ subtrahieren resp. addieren.

Zwischen beiden unterschiedenen Fällen liegt der noch übrige dritte: $m = n$, den man als gemeinsamen Grenzfall jener ansehen kann. Da $z + n$ aus z durch successive Hinzufügung von n Einheiten und hieraus $(z + n) - n$ durch successive Wegnahme eben dieser Einheiten entsteht, so ist offenbar $(z + n) - n = z$. Indem man daher zur Definition des Zeichens $n - n$ jede der beiden Formeln (1) oder (2) verwendet, findet man

$$z + (n - n) = z = z - (n - n). \tag{5}$$

Man nennt diese Differenz die Null, in Zeichen 0; die vorstehende Formel lehrt mithin, dafs eine Zahl, wenn man die Null ihr hinzufügt oder sie von ihr wegnimmt, ungeändert bleibt.

Nachdem diese Begriffe gewonnen worden sind, würde nunmehr eine erschöpfende Darstellung zu entwickeln haben, wie die definierten negativen Zahlen und die Null mit den positiven sowie unter sich selbst durch Addition, Subtraktion und Multiplikation zu verbinden sind. Bei der Herleitung dieser Regeln hätte man stets zu beachten, dafs diese Zahlen im Grunde nicht an sich, sondern immer nur zugleich mit andern existieren, mit denen sie durch Addition oder Subtraktion verbunden sind. Wir beschränken uns hier darauf, beispielsweise darzuthun, wie das Produkt aus einer positiven Zahl μ in eine negative Zahl $-\nu = -(n - m)$, wo $m < n$ gedacht ist, gedeutet werden mufs. Den Definitionen zufolge ist $\nu = n - m$ und für eine hinreichend grofse Zahl z

$$\mu(z + (m - n)) = \mu((z + m) - n); \tag{6}$$

also ist $n = \nu + m$ und folglich, wie einfach zu erkennen,

$$(z + m) - (\nu + m) = z - \nu,$$

$$\mu(z - \nu) = \mu z - \mu\nu.$$

Die Formel (6) nimmt daher die Gestalt an:

$$\mu(z + (m - n)) = \mu z - \mu\nu$$

oder

$$\mu(z + (-\nu)) = \mu z - \mu\nu.$$

Will man nun, dafs der Rechnung die wichtige Eigenschaft der Distribuitivität, welche der Multiplikation positiver Zahlen zukommt, auch bei Zulassung negativer Zahlen gewahrt bleibe, so hat man die linke Seite dieser Formel durch $\mu z + \mu(-\nu)$ zu ersetzen und zu erschliefsen, dafs

$$\mu(-\nu) = -\mu\nu$$

ist. Aus ähnlichen Erwägungen leitet man die übrigen der bekannten Regeln für die Multiplikation beliebiger, positiver oder negativer Zahlen her, die sich in den vier folgenden Gleichungen aussprechen:

$$\left\{\begin{aligned} \mu\cdot(-\nu) &= (-\mu)\cdot\nu &&= -\mu\nu \\ \mu\cdot\nu &= (-\mu)\cdot(-\nu) &&= +\mu\nu. \end{aligned}\right. \tag{7}$$

Wir beschliefsen diese einleitenden Betrachtungen, indem wir die Gröfsenordnung der negativen Zahlen fixieren. Ist $m-n=\nu$ eine positive Zahl, so ist $m=\nu+n$ und $m+1=(\nu+n)+1=(\nu+1)+n$, folglich $(m+1)-n=\nu+1$. Für eine hinreichend grofse Zahl z bestehen demnach die Formeln:

$$z-\nu = z+(n-m),$$
$$z-(\nu+1) = z+[n-(m+1)]$$

und aus ihnen erschliefst man successive die folgenden:

$$\begin{aligned} [z-(\nu+1)]+1 &= (z+[n-(m+1)])+1 = [z+n-(m+1)]+1 \\ &= 1+[z+n-(m+1)] = (1+z+n)-(m+1) = (z+n)-m \\ &= z+(n-m) = z-\nu, \end{aligned}$$

ein Resultat, demzufolge wir aussagen können: Die negative Zahl $-\nu$ entstehe durch additive Verknüpfung der negativen Zahl $-(\nu+1)$ mit der Einheit, wodurch dann in Analogie mit den positiven Zahlen die negative Zahl $-\nu$ als die auf $-(\nu+1)$ folgende oder nächstgröfsere Zahl zu betrachten ist. Da die vorstehende Überlegung auch für den Grenzfall $\nu=0$ in Giltigkeit bleibt, so ist die „Zahl“ Null als die auf -1 folgende, nächst gröfsere Zahl anzusehen; und da durch Ausdehnung der Kommutativität der Summation auch auf den Fall, wo einer der Summanden die Null ist, sich

$$0+1=1+0=1$$

findet, so ist die Zahl 1 als die auf 0 folgende oder nächst gröfsere ganze Zahl zu betrachten. Somit erhalten wir bei Zulassung der Null und der negativen Zahlen an Stelle der ursprünglichen, sogenannten natürlichen Reihe (K) der ganzen Zahlen jetzt die umfassendere der Gröfse nach geordnete Zahlenreihe (Z):

$$\cdots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ \cdots, \tag{Z}$$

welche nach beiden Richtungen hin unbegrenzt fortgesetzt werden kann. Diese Zahlenreihe (Z) bildet das Material, dessen Eigenschaften die Theorie der ganzen Zahlen zur Erörterung bringt.

Zweites Kapitel.

Von der Teilbarkeit der Zahlen.

1. Aus den im vorigen Kapitel begründeten Regeln zur Addition, Subtraktion und Multiplikation von Zahlen folgt offenbar für die Zahlenreihe

$$(Z) \qquad \cdots, -3, -2, -1, 0, 1, 2, 3, 4, 5, \cdots$$

die Eigenschaft, dafs die Summe, die Differenz und das Produkt aus einer beliebigen und einer gleichfalls beliebigen Zahl dieser Reihe, mag sie der ersteren gleich oder davon verschieden sein, wieder eine Zahl derselben Reihe sein mufs; mit andern Worten: die Zahlen jener Reihe reproduzieren sich durch Addition, Subtraktion und Multiplikation. Aus solcher Rücksicht nennt man (nach Dedekind) die Zahlenreihe (Z) ein Zahlensystem.

Sei nun n irgend eine (positive) ganze Zahl; dann werden die Produkte

$$(1) \qquad \cdots, -3n, -2n, -n, 0, n, 2n, 3n, 4n, 5n, \cdots,$$

welche durch Multiplikation dieser Zahl mit den Zahlen der Reihe (Z) entstehen, sämtlich verschiedene Zahlen der letzteren sein; doch enthält nicht auch umgekehrt die Reihe (1) die sämtlichen Zahlen der Reihe (Z); denn, um in der letzteren von einem jener Produkte zum nächstfolgenden, etwa von qn zu $(q+1)n$ zu gelangen, mufs man mit qn die Einheit n-mal durch Addition verknüpfen, sodafs zwischen qn und $(q+1)n$ noch die $n-1$ anderen Zahlen

$$(2) \qquad qn+1, \; qn+2, \; \ldots, \; qn+(n-1)$$

enthalten sind. Fügt man jedoch die zwischen je zwei aufeinanderfolgenden Produkten der Reihe (1) enthaltenen Zahlen dieser Reihe hinzu, so entsteht die gesamte Reihe (Z) und somit darf man sagen:

Ist m irgend eine Zahl der Reihe (Z), so hat sie, bezüglich einer bestimmten (positiven) Zahl n dieser Reihe betrachtet, notwendig **die Form:**

$$(3) \qquad m = qn + r,$$

worin unter q eine Zahl der Reihe (Z), unter r eine der Zahlen $0, 1, 2, \ldots, n-1$ zu verstehen ist. Diese einfache Bemerkung ist als der Ausgangspunkt aller ferneren Entwicklungen und somit (wie Dedekind, Vorlesungen über Zahlentheorie von Dirichlet, 4. Aufl. p. 514, Anmerkung, mit Recht hervorgehoben hat) als die Grundlage der gesamten Zahlentheorie zu betrachten.

Ist $r = 0$, gehört nämlich m der Reihe (1) an, so heifst m ein Vielfaches von n; jedes Vielfache von n hat mithin die Form qn

und sie werden aus dieser Form sämtlich erhalten, wenn man für q jede der Zahlen (Z) setzt oder q diese Zahlenreihe durchlaufen läfst. Umgekehrt nennt man, wenn m ein Vielfaches von n ist, n einen Teiler oder Divisor von n. Als solcher würde der Formel $m = qn = nq$ gemäfs auch die Zahl q zu bezeichnen sein und man heifst sie so den zu n komplementären Teiler von m; wenn man jedoch n als Teiler von m hervorhebt, so nennt man q den ihm entsprechenden Quotienten und deutet ihn an durch das Zeichen:

$$q = \frac{m}{n}. \tag{4}$$

Das solcherweise definierte Zeichen $\frac{m}{n}$ ist von vornherein ohne Bedeutung, wenn m kein Vielfaches von n ist, mithin r in der Formel (3) sich von 0 unterscheidet. Um ihm auch in diesem Falle eine Bedeutung zu verleihen, kann man es überhaupt als den Ausdruck des gegenseitigen numerischen Verhaltens der beiden Zahlen m, n, wie es in jener Formel ausgesprochen ist, definieren. Dann deuten wir also durch das sogenannte Bruchzeichen $\frac{m}{n}$ einfach das Stattfinden der Gleichung (3) unter den für q und r angegebenen Bedingungen an; die Gleichung (4) aber wäre nur eine Konsequenz dieses Stattfindens für den Fall, in welchem m ein Vielfaches von n ist. Es würde sich alsdann fragen, in welcher Weise man mehrere solche Zeichen, wie Zahlen, durch die einfachsten Operationen der Addition, Subtraktion und Multiplikation mit einander zu verbinden habe. Seien also zwei Brüche $\frac{m}{n}, \frac{m'}{n'}$ gegeben d. h. zwei Beziehungen von der Form:

$$m = qn + r, \quad m' = q'n' + r', \tag{5}$$

wo q, q' Zahlen der Reihe (Z), r eine der Zahlen $0, 1, 2, \ldots, n-1$ und r' eine der Zahlen $0, 1, 2, \ldots, n'-1$ bedeuten; man folgert hieraus die folgende;

$$mn' \pm m'n = \mathfrak{q} \cdot nn' + \mathfrak{r}, \tag{6}$$

wo

$$rn' \pm r'n = knn' + \mathfrak{r}, \quad \mathfrak{q} = q \pm q' + k$$

gesetzt und unter k eine Zahl der Reihe (Z), unter $\mathfrak{r}$ eine solche der Reihe $0, 1, 2, \ldots, nn'-1$ verstanden ist. Wie nun den Gleichungen (5) die Brüche $\frac{m}{n}, \frac{m'}{n'}$ resp., so entspricht der Gleichung (6) der Bruch $\frac{mn' \pm m'n}{nn'}$. Falls aber q, q' den Quotienten $\frac{m}{n}, \frac{m'}{n'}$ gleich, nämlich r, r' gleich 0 sind, ist auch sowohl $\mathfrak{r}$ wie k gleich 0; des erstern Umstandes willen wird $\mathfrak{q}$ zum Quotienten $\frac{mn' \pm m'n}{nn'}$, des

letzteren willen ist $\mathfrak{q} = q \pm q'$, d. i. dieser Quotient ist die Summe resp. die Differenz der Quotienten $\frac{m}{n}$, $\frac{m'}{n'}$, in Zeichen:

$$(7) \qquad \frac{mn' \pm m'n}{nn'} = \frac{m}{n} \pm \frac{m'}{n'}.$$

Aus diesem Grunde nimmt man allgemein die letztere Gleichung zur **Definition** der Summe resp. der Differenz der beiden **Brüche** $\frac{m}{n}$, $\frac{m'}{n'}$.

Ähnlicherweise folgt aus den Beziehungen (5) die neue:

$$(8) \qquad mm' = \mathfrak{q}nn' + \mathfrak{r},$$

wobei

$$qnr' + q'n'r + rr' = knn' + \mathfrak{r}, \qquad \mathfrak{q} = qq' + k$$

gesetzt und unter k eine Zahl der Reihe (Z), unter $\mathfrak{r}$ eine Zahl der Reihe $0, 1, 2, \ldots, nn' - 1$ verstanden ist. Der Gleichung (8) entspricht das Bruchzeichen $\frac{mm'}{nn'}$. Sind aber q, q' die Quotienten $\frac{m}{n}$, $\frac{m'}{n'}$, d. i. $r = r' = 0$, so ist auch $\mathfrak{r} = 0$, $k = 0$, also $\mathfrak{q}$ der Quotient $\frac{mm'}{nn'}$ und dieser Quotient gleich qq' d. i. gleich dem Produkte der Quotienten $\frac{m}{n}$, $\frac{m'}{n'}$, in Zeichen:

$$(9) \qquad \frac{mm'}{nn'} = \frac{m}{n} \cdot \frac{m'}{n'}.$$

Daher **definiert** man auch allgemein durch diese Gleichheit das Produkt der beiden **Brüche** $\frac{m}{n}$, $\frac{m'}{n'}$.

Die Zahl q in der Formel (3), welche in dem Falle, wo m ein Vielfaches von n ist, der bezügliche Quotient $\frac{m}{n}$ hiefs, wird allgemein das gröfste Ganze von m in Bezug auf n oder das gröfste in dem Bruche $\frac{m}{n}$ enthaltene Ganze genannt. Die Zahl r heifst der Rest von m mit Bezug auf n. Zur Bezeichnung des gröfsten Ganzen im Bruche $\frac{m}{n}$ (des *Entier* von $\frac{m}{n}$) hat Legendre (s. seine *théorie des nombres*, introduction) das Funktionszeichen $E\left(\frac{m}{n}\right)$ eingeführt, doch erscheint es bei ihm wesentlich auf den Fall positiver Werte des Argumentes $\frac{m}{n}$ bezogen. Statt dessen bezeichnete Gaufs (*Werke II*, p. 5, 1808) mit $[x]$ für jeden reellen, positiven oder negativen Wert von x die algebraisch gröfste darin enthaltene ganze Zahl, sodafs in algebraischem Sinne immer

$$(10) \qquad [x] \gtreqless x < [x] + 1$$

ist; demzufolge ist $\left[\frac{m}{n}\right]$ gleichbedeutend mit der Zahl q in der Formel (3) oder mit dem Zeichen $E\left(\frac{m}{n}\right)$, wenn dies für jeden beliebigen, positiven wie negativen Bruch $\frac{m}{n}$ gebraucht wird.

2. Ist $m = qn$, so ist auch $m = (-q) \cdot (-n)$ d. h., wenn n ein Teiler einer Zahl ist, so ist's auch die entgegengesetzte Zahl $-n$. Desgleichen folgt aus $m = qn$ auch $-m = (-q) \cdot n$ d. h. entgegengesetzte Zahlen haben stets die nämlichen Teiler. Aus diesem Grunde darf man sich bei der Untersuchung der Teiler von Zahlen durchaus auf positive Zahlen beschränken.

Sind dann m, m' zwei verschiedene Vielfache von n:

$$m = qn, \quad m' = q'n,$$

so heifst n ein gemeinschaftlicher Teiler von m, m'. Zwei Zahlen haben stets die Einheit zu einem gemeinsamen Teiler, da jede Zahl m als Vielfaches der Einheit $m = m \cdot 1$ aufgefafst werden kann. Ist ihnen aber aufser diesem selbstverständlichen Teiler kein anderer Teiler gemeinsam, so heifsen sie teilerfremd, Zahlen ohne gemeinsamen Teiler oder auch relativ prim.

Da $m = 1 \cdot m$, so ist m selbst ein Teiler von m. Jeder von m verschiedene Teiler von m aber ist kleiner als m, denn m ist eine Summe aus einer Anzahl Summanden, deren jeder gleich jenem Teiler ist. Da hiernach nicht nur sämtliche Teiler von m, sondern umsomehr alle diejenigen, die m und einer andern Zahl m' gemeinsam sind, Zahlen des Abschnittes $|1, 2, 3, \ldots, m|$ sind, so giebt es unter den gemeinsamen Teilern von m, m' einen gröfsten gemeinsamen Teiler. Wird dieser δ genannt und

$$m = \delta\mu, \quad m' = \delta\mu'$$

gesetzt, so sind μ, μ' zwei relativ prime Zahlen. Denn, hätten sie einen von 1 verschiedenen gemeinsamen Teiler d, sodafs man $\mu = d\nu$, $\mu' = d\nu'$ setzen könnte, so folgte $m = d\delta\nu$, $m' = d\delta\nu'$ und die beiden Zahlen m, m' hätten den gemeinsamen Teiler $d\delta$, welcher als Vielfaches von δ gröfser wäre als δ, gegen die Bedeutung dieses Buchstabens.

Nun haben die Zahlen (1), ebenso wie die Zahlen (Z), deren Reihe als der $n = 1$ entsprechende besondere Fall der Reihe (1) angesehen werden kann, die Eigenschaft, dafs die Summe und die Differenz aus einer beliebigen Zahl der Reihe (1) und einer gleichfalls beliebigen Zahl derselben, mag sie die gleiche sein wie die erstere, oder nicht, wieder eine Zahl der Reihe (1) ist; denn aus qn und $q'n$ folgt

$$qn \pm q'n = (q \pm q')\,n \tag{11}$$

d. h. gleich einem Vielfachen von n. Derartige Zahlenmengen kommen in der Zahlentheorie sehr häufig in Betracht und werden deshalb (nach Dedekind und Kronecker) durch ein besonderes Wort, nämlich als Moduln gekennzeichnet. Wir denken uns irgend einen aus Zahlen der Reihe (Z) gebildeten Modulus. Jedenfalls enthält ein solcher auch positive Zahlen; denn, enthält er die negative Zahl $-m$, so kommt auch die Zahl $-m-(-m)=0$ und folglich auch die Zahl $0-(-m)=+m$ darin vor[1]. Wenn diese Zahl m nicht die kleinste im Modulus enthaltene positive Zahl ist, so enthält der Abschnitt $|1, 2, 3, \ldots, m|$ noch andere darin auftretende Zahlen und unter ihnen ist eine die kleinste. Sei diese Zahl n. Dann enthält der Modulus alle Vielfachen von n d. h. alle Zahlen von der Form nz, wo unter z jede beliebige Zahl der Reihe (Z) verstanden wird; aber er kann auch keine andere Zahl weiter enthalten. Denn, wäre $m=qn+r$, wo r von 0 verschieden, also eine der Zahlen $1, 2, 3, \ldots, n-1$ ist, im Modulus enthalten, so wäre es auch, der Bedeutung eines solchen gemäfs, die positive Zahl

$$(qn+r)-qn=r,$$

welche doch kleiner wäre als n. Man gelangt also zu dem

Satz I. Jeder aus den Zahlen (Z) gebildete Modulus besteht aus den Zahlen nz, wo z jede der Zahlen (Z), n aber die kleinste positive Zahl bedeutet, welche der Modulus enthält. Man bezeichnet ihn demnach kurz mit (nz).

Seien nun a, b zwei gegebene (positive) Zahlen; ihnen entsprechen zwei Moduln (ax), (by) aus der Reihe (Z). Der Ausdruck $ax+by$ giebt dann auch eine Zahl derselben Reihe, wenn für x, y irgend welche ganze Zahlen gesetzt werden. Die Gesamtheit aller Zahlen von dieser Form ist ebenfalls ein Modulus; in der That geben zwei Zahlen $ax'+by'$, $ax''+by''$ der Gesamtheit die Summe bezw. die Differenz

$$(ax'+by')\pm(ax''+by'')=a(x'\pm x'')+b(y'\pm y'')$$

d. i. wieder eine Zahl derselben Gesamtheit. Ist demnach n die kleinste positive Zahl in der letzteren, so ist jede Zahl derselben ein Vielfaches von n, und da insbesondere a, b selbst Zahlen der Gesamtheit sind, so sind auch sie Vielfache von n oder n ist ein gemeinsamer Teiler von a, b. Andererseits mufs der Ausdruck $ax+by$ für gewisse Werte ξ, η von x, y der Zahl n gleich werden:

$$a\xi+b\eta=n. \tag{12}$$

---

1) Von der Zahlenmenge — wenn man so sagen will —, die nur aus der Zahl 0 besteht und, wie sogleich zu sehen, die Eigenschaft eines Modulus besitzt, wird von uns im Folgenden gänzlich abgesehen.

Da nach (11) jeder gemeinsame Teiler zweier Zahlen auch Teiler ihrer Summe und ihrer Differenz ist, so ist der vorstehenden Gleichung zufolge jeder gemeinsame Teiler von a, b, also auch ihr gröfster gemeinsamer Teiler δ ein Teiler von n, mithin $n = d\delta$, der gemeinsame Teiler n von a, b wäre also gröfser als ihr gröfster gemeinsamer Teiler, wenn d von 1 verschieden wäre, und deshalb mufs $d = 1$ also $n = \delta$ sein. Wir sind auf diese Weise zu folgenden Sätzen geführt worden:

Satz II. Die Gesamtheit der Zahlen $ax + by$ ist ein Modulus (δz), in welchem δ der gröfste gemeinsame Teiler von a, b ist; jene Gesamtheit darf deshalb der gröfste gemeinsame Teiler der Moduln (ax), (by) genannt werden.

Satz III. Haben zwei Zahlen a, b den gröfsten gemeinsamen Teiler δ, so giebt es Zahlen ξ, η, welche der Gleichung

$$a\xi + b\eta = \delta \tag{13}$$

Genüge leisten.

Satz IV. Jeder gemeinsame Teiler von a, b ist demnach ein Teiler ihres gröfsten gemeinsamen Teilers δ. Das Umgekehrte leuchtet von selbst ein. Die gemeinsamen Teiler zweier Zahlen sind mithin identisch mit den Divisoren ihres gröfsten gemeinschaftlichen Teilers.

Satz V. Sind insbesondere a, b relativ prime Zahlen, für welche $\delta = 1$ ist, so besteht für gewisse ganzzahlige Werte ξ, η die Gleichung

$$a\xi + b\eta = 1. \tag{14}$$

Dies Resultat ist von hervorragender Wichtigkeit und liefert sogleich die fundamentalsten Sätze über Teilbarkeit der Zahlen. Ist nämlich c irgend eine dritte Zahl, so folgt aus (14)

$$ac\xi + bc\eta = c.$$

Ist daher d ein gemeinsamer Teiler von ac und b, so mufs er es auch sein von c oder:

Satz VI. Ein Produkt, dessen einer Faktor prim ist zu einer Zahl, kann nur dann einen Teiler mit dieser Zahl gemein haben, wenn der andere Faktor ihn hat. Insbesondere ist das Produkt durch jene Zahl nur dann teilbar, wenn der andere Faktor durch sie teilbar ist.

Sind nun nicht nur a, b, sondern auch c, b relativ prime Zahlen, so kann ein gemeinsamer Teiler d von ac und b, da er Teiler von c, also gemeinsamer Teiler von b, c sein müfste, nur gleich 1 sein, und folglich müssen auch ac und b Zahlen ohne gemeinsamen Teiler sein. Man findet also

Satz VII. Das Produkt von (zwei) Zahlen, deren jede relativ prim ist gegen eine gegebene Zahl, ist es gegen diese Zahl gleichfalls.

Allgemeiner: Ist jede der Zahlen $a, b, c, \ldots$ relativ prim gegen jede der Zahlen $a', b', c', \ldots$, so ist auch das Produkt $abc\ldots$ prim gegen das Produkt $a'b'c'\ldots$; denn zunächst folgert man aus dem vorigen Satze, dafs das erstere Produkt prim ist gegen jede der Zahlen $a', b', c', \ldots$ und folglich wieder das Produkt der letzteren Zahlen gegen jenes Produkt. Sind mithin a, a' relativ prime Zahlen, so ist auch jede Potenz von a prim gegen jede Potenz von a'.

3. Auch unter den gemeinsamen Teilern mehrerer, etwa ν Zahlen

$$m, n, p, q, r, \ldots \tag{15}$$

mufs einer der gröfste sein. Der Natur der Sache nach ist er unabhängig von dem Wege, auf dem wir ihn bestimmen können, insbesondere also von der Reihenfolge, in welcher wir zu diesem Zwecke die gegebenen Zahlen mit einander verknüpfen. Sei nun δ der gröfste gemeinsame Teiler von m, n, so mufs jede Zahl, welche zugleich in jeder der gegebenen Zahlen aufgeht, auch ein Teiler von δ, also ein gemeinsamer Teiler der Zahlen

$$\delta, p, q, r, \ldots \tag{16}$$

sein, deren Anzahl um Eins geringer ist als die der gegebenen Zahlen; und umgekehrt ist jeder gemeinsame Teiler dieser neuen Zahlenreihe, da er in δ also zugleich auch in m, n aufgeht, auch ein solcher für die gegebene Reihe von Zahlen. Gesetzt nun, es stünde bereits fest, dafs die gemeinsamen Teiler der Reihe (16) von $\nu - 1$ Zahlen mit den Divisoren ihres gröfsten gemeinsamen Teilers Δ übereinstimmen, so würden auch die gemeinsamen Teiler der Zahlen (15) d. i. von ν Zahlen die Teiler von Δ und demnach Δ selbst der gröfste gemeinsame Teiler der Zahlen (15) sein. Dies gilt aber in der That, da es für zwei beliebige Zahlen bereits bewiesen ist. Man hat mithin im Vorstehenden nicht nur eine Methode, die Aufsuchung des gröfsten gemeinsamen Teilers von ν Zahlen auf diejenige für $\nu - 1$, dann für $\nu - 2$ u. s. w., endlich auf die für zwei Zahlen zurückzuführen, sondern gewinnt auch den Satz: Die gemeinsamen Teiler mehrerer Zahlen stimmen mit den Divisoren ihres gröfsten gemeinsamen Teilers überein.

Ist nun Δ der gröfste gemeinsame Teiler der Zahlen (15), sodafs man setzen darf

$$m = \Delta m', \quad n = \Delta n', \quad p = \Delta p', \quad q = \Delta q', \quad r = \Delta r', \ldots,$$

so können offenbar $m', n', p', q', r', \ldots$ keinen Teiler mehr gemein

haben, sie sind Zahlen ohne gemeinsamen Teiler, insgesamt relativ prim.

Von diesem Falle ist der andere wohl zu unterscheiden, in welchem sie zu je zweien relativ prim sind; denn zwar sind in ihm ersichtlich die Zahlen (15) auch insgesamt ohne gemeinsamen Teiler, es braucht aber nicht umgekehrt zu sein; denn z. B. wären m, n, p drei Zahlen ohne gemeinsamen Teiler, wenn m, n einzeln zu p prim wären, doch unter einander einen gemeinsamen Teiler besäſsen. —

Wir schlieſsen hier mit einer Betrachtung ab, welche von Dedekind (*Braunschweiger Festschrift* 1897, p. 1) zum Ausgangspunkte für Untersuchungen einer sehr viel höheren Art genommen worden ist. Seien m, n, p drei gegebene Zahlen, $\varDelta$ ihr gröſster gemeinsamer Teiler, sodaſs man

$$m = \varDelta m', \quad n = \varDelta n', \quad p = \varDelta p'$$

setzen kann, wo dann m', n', p' Zahlen ohne gemeinsamen Teiler sind. Bezeichnen wir mit m'', n'', p'' die gröſsten gemeinsamen Teiler je zweier dieser Zahlen, nämlich resp. von n', p'; p', m'; m', n'; so werden sie zu je zweien prim sein und Gleichungen bestehen von folgender Gestalt:

$$\begin{array}{ccc} \times & n' = m''n_1, & p' = m''p_1, \\ m' = n''m_2, & \times & p' = n''p_2, \\ m' = p''m_3, & n' = p''n_3, & \times \end{array}$$

in denen $n_1, p_1, m_2, p_2, m_3, n_3$ ganze Zahlen sind. Aus der Gleichheit $n''m_2 = p''m_3$ folgt daher

$$m_2 = \mu'p'', \quad m_3 = \mu'n'',$$

aus den Gleichheiten $p''n_3 = m''n_1$, $m''p_1 = n''p_2$ ähnlicherweise

$$n_3 = \nu'm'', \quad n_1 = \nu'p'',$$
$$p_1 = \pi'n'', \quad p_2 = \pi'm'',$$

wo μ', ν', π' ganze Zahlen sind. Hiernach findet sich

$$m' = \mu'n''p'', \quad n' = \nu'p''m'', \quad p' = \pi'm''n''$$

und

$$m = \varDelta\mu'n''p'', \quad n = \varDelta\nu'p''m'', \quad p = \varDelta\pi'm''n''.$$

Da n_1, p_1; m_2, p_2; m_3, n_3 paarweise relativ prim sind, ergeben sich μ', ν', π' zu je zweien, auſserdem resp. zu m'', n'', p'' relativ prim. Diese Darstellung der drei Zahlen m, n, p als Produkte aus ihrem gröſsten gemeinsamen Teiler und den sechs anderen Zahlen μ', ν', π', m'', n'', p'' nennt Dedekind die Zerlegung derselben in ihre **Kerne.**

4. Sind m, m' zwei gegebene Zahlen, so heifst jede Zahl, welche sowohl ein Vielfaches von m als auch von m' ist, ein gemeinsames Vielfaches von m, m'. Es ist leicht eine Formel aufzustellen, welche diese sämtlichen gemeinsamen Vielfachen darstellt. Sei nämlich δ der gröfste gemeinsame Teiler von m, m', sodafs man

$$m = \delta\mu, \quad m' = \delta\mu'$$

setzen darf, wo nun μ, μ' relativ prime Zahlen bedeuten, so ist zunächst jedes Vielfache von m von der Form mz, unter z jede Zahl der Reihe (Z) verstanden. Soll diese Zahl $mz = \delta\mu z$ aber durch $m' = \delta\mu'$ oder, was auf dasselbe hinauskommt, μz durch μ' teilbar sein, so mufs z es sein, etwa $z = \mu' z'$, und somit

$$mz = \delta\mu\mu' z' = \frac{mm'}{\delta} \cdot z'$$

sein. Jedes gemeinsame Vielfache von m, m' ist demnach ein Vielfaches der Zahl $\frac{mm'}{\delta}$. Da umgekehrt

$$\frac{mm'}{\delta} \cdot z' = m \cdot \mu' z' = m' \cdot \mu z'$$

gesetzt werden kann, also jedes Vielfache von $\frac{mm'}{\delta}$ auch gemeinsames Vielfache von m, m' ist, so stimmen die gemeinsamen Vielfachen dieser beiden Zahlen mit den Vielfachen von $\frac{mm'}{\delta}$ überein, und unter diesen ist $\frac{mm'}{\delta}$ das kleinste. Man erhält demnach das kleinste gemeinsame Vielfache zweier Zahlen, wenn man deren Produkt durch ihren gröfsten gemeinsamen Teiler dividiert. Das kleinste gemeinsame Vielfache zweier relativ primer Zahlen (für welche $\delta = 1$ wäre) ist ihrem Produkte gleich.

Auch für mehrere, etwa ν Zahlen:

$$m, n, p, q, r, \ldots \tag{17}$$

wird es ein kleinstes gemeinsames Vielfache geben, welches der Natur der Sache nach unabhängig ist von dem Wege, auf welchem wir es suchen, insbesondere von der Reihenfolge, in der wir hierbei jene Zahlen verknüpfen. Sei nun μ das kleinste gemeinsame Vielfache von m, n, so wird jede Zahl, welche durch die Zahlen (17) einzeln teilbar ist, auch ein gemeinsames Vielfache der Zahlen

$$\mu, p, q, r, \ldots \tag{18}$$

sein, deren Anzahl $\nu - 1$ ist; und umgekehrt mufs jedes gemeinsame Vielfache der letztern, da es ein Vielfaches von μ ist, auch ein solches von m und n, d. i. ein gemeinsames Vielfache der Zahlen (17) sein. Nimmt man daher als bereits feststehend an, dafs die gemein-

samen Vielfachen der Zahlen (18) mit den Vielfachen ihres kleinsten gemeinsamen Vielfachen M identisch sind, so werden auch die gemeinsamen Vielfachen der Zahlen (17) die Vielfachen von M, das kleinste gemeinsame Vielfache derselben also die Zahl M selbst sein. Dies gilt aber in der That, denn für zwei beliebige Zahlen ist es bereits bewiesen. So führt die vorstehend angedeutete Betrachtung die Bestimmung des kleinsten gemeinsamen Vielfachen mehrerer Zahlen auf diejenige für zwei Zahlen zurück und liefert zudem den Satz: Die gemeinsamen Vielfachen mehrerer Zahlen stimmen mit den sämtlichen Vielfachen ihres kleinsten gemeinsamen Vielfachen überein.

Sind die Zahlen m, n der Reihe (17) relativ prim, so wird $\mu = mn$; also ist in diesem Falle das kleinste gemeinsame Vielfache der Zahlen (17) mit demjenigen der Zahlen

$$mn, p, q, r, \ldots$$

identisch; sind nun die Zahlen (17) durchweg zu je zweien, also auch m sowie n und folglich auch mn zu p relativ prim, so wird wieder das kleinste gemeinsame Vielfache der letzteren Reihe mit demjenigen der neuen Reihe

$$mnp, q, r, \ldots$$

übereinstimmen, u. s. w. Man findet demnach schliefslich den Satz: Das kleinste gemeinsame Vielfache von Zahlen, die zu je zweien relativ prim sind, ist gleich ihrem Produkte; daher ist eine Zahl, welche durch jede dieser Zahlen teilbar ist, auch teilbar durch deren Produkt.

Sei P das Produkt der Zahlen (17). Der gröfste gemeinsame Teiler der ganzen Zahlen

$$\frac{\mathsf{M}P}{m}, \frac{\mathsf{M}P}{n}, \frac{\mathsf{M}P}{p}, \ldots$$

ist ersichtlich sowohl M-mal dem gröfsten gemeinsamen Teiler der ganzen Zahlen

$$\frac{P}{m}, \frac{P}{n}, \frac{P}{p}, \ldots$$

als auch P-mal dem gröfsten gemeinsamen Teiler der ganzen Zahlen

$$\frac{\mathsf{M}}{m}, \frac{\mathsf{M}}{n}, \frac{\mathsf{M}}{p}, \ldots.$$

Nun ist aber der letztere gleich 1; denn, nennen wir ihn d, so wird $\frac{\mathsf{M}}{d}$ durch jede der Zahlen $m, n, p, \ldots$ teilbar sein und daher auch durch ihr kleinstes gemeinsames Vielfache d. i. durch M aufgehen, mithin mufs $d = 1$ sein. So ergiebt sich der fernere Satz: Das Produkt von ν Zahlen ist gleich ihrem kleinsten gemein-

samen Vielfachen, multipliziert in den gröſsten gemeinsamen Teiler der aus je $\nu - 1$ der Zahlen gebildeten Produkte.

Andere Beziehungen ähnlicher Art s. bei Lucas, *théorie des nombres*, 1891, p. 345, 346. —

5. Die bereits von Euclid (*Elementa*, lib. VII) gegebenen Fundamentalsätze der Nr. 2 führen nun leicht zu dem Hauptsatze von der Zerlegbarkeit der Zahlen in einfachste Faktoren. Hierbei darf man sich wieder auf die Betrachtung positiver Zahlen beschränken, da aus ihnen die negativen durch Hinzufügung des Zeichens — hervorgehen.

Die (positiven) Zahlen dürfen unterschieden werden in zusammengesetzte oder zerlegbare und in unzerlegbare Zahlen m, jenachdem es möglich ist, m als Produkt zweier Faktoren darzustellen, deren jeder von 1 verschieden ist, oder nicht; die unzerlegbaren Zahlen haben, mit anderen Worten, keinen weiteren Teiler, als die Einheit und sich selbst, während den zusammengesetzten Zahlen noch andere Teiler eigen sind. Wir verstehen ferner unter einer Primzahl eine Zahl p, welcher die Eigenschaft zukommt, daſs jedes Produkt ab zweier Zahlen nur dann durch p teilbar ist, wenn a oder b es ist. Aus dieser Definition folgt, daſs p unzerlegbar ist; denn, wäre $p = q \cdot r$, so wären die von der Einheit verschiedenen Faktoren q, r kleiner als p und deshalb jedenfalls nicht teilbar durch p; mithin würde das Produkt ab, indem man $a = q$, $b = r$ wählt, gegen die Bedeutung einer Primzahl durch p teilbar sein, ohne daſs a oder b es wäre. Aber auch umgekehrt ist jede unzerlegbare Zahl p eine Primzahl; denn, da diese unzerlegbare Zahl keine Teiler besitzt als 1 und p, so kann, wenn ab durch p teilbar ist, a, wenn es nicht durch p aufgeht, nur relativ prim gegen p sein und dann müſste dem Satze VI der Nr. 2 zufolge b durch p teilbar sein. Hiernach sind Primzahlen und unzerlegbare Zahlen identisch; aber es schien angezeigt, sie von vornherein in der Definition auseinander zu halten, da diese Identität in der allgemeineren Theorie der Zahlen, der Theorie der „ganzen algebraischen" Zahlen, nicht durchweg mehr ebenso besteht.

Wenn nun m eine zusammengesetzte Zahl ist, so giebt es wenigstens einen Teiler m' derselben, der von 1 und m verschieden also kleiner als m ist, und da überhaupt alle Teiler von m Zahlen des Abschnittes $|1, 2, 3, \ldots, m|$ sind, muſs einer von allen Teilern dieser Art der kleinste sein; er heiſse p. Diese Zahl ist unzerlegbar; denn, wäre p' ein von 1 und p verschiedener Teiler von p also kleiner als p, so hätte auch m diesen Teiler $p' < p$, gegen die Bedeutung dieses Zeichens. Mithin hat jede zusammengesetzte Zahl m einen Primteiler p, sodaſs man setzen darf $m = p \cdot m_1$, wo m_1 eine ganze Zahl, welche als Teiler von m, da p von 1 verschieden ist,

kleiner als m sein mufs. Ist diese Zahl noch zusammengesetzt, so darf man ähnlich setzen: $m_1 = p_1 m_2$, wo p_1 eine möglicherweise mit p gleiche Primzahl, m_2 eine ganze Zahl kleiner als m_1 ist, u. s. w. In der Reihe der abnehmenden Zahlen $m, m_1, m_2, \ldots,$ auf welche man so stöfst und die sämtlich dem Abschnitte $|1, 2, 3, \ldots, m|$ angehörig sind, mufs eine kleinste m_ν vorhanden sein und diese ergiebt sich dann, ähnlich wie p, als unzerlegbar d. i. als eine Primzahl p_ν. Hiernach findet man die Formeln:

$$m = pm_1, \quad m_1 = p_1 m_2, \cdots, m_{\nu-1} = p_{\nu-1} \cdot p_\nu$$

und folglich

$$m = pp_1p_2 \cdots p_{\nu-1}p_\nu \tag{19}$$

d. h. eine Zerlegung der zusammengesetzten Zahl m in lauter Primzahlfaktoren.

Ist somit die Möglichkeit solcher Zerlegung einer zusammengesetzten Zahl erwiesen, so ist es sehr wesentlich, zu zeigen, dafs sie nur auf eine Weise möglich ist. Gäbe es aber noch eine zweite Zerlegung der Zahl m in Primfaktoren, nämlich

$$m = q_1 q_2 q_3 \cdots q_\mu, \tag{20}$$

so müfste

$$p_1 p_2 \cdots p_\nu = q_1 q_2 \cdots q_\mu \tag{21}$$

sein. Da hiernach die rechte Seite der Gleichung durch den Primfaktor p_1 der linken Seite teilbar ist, müfste einer der Primfaktoren q es sein, was, weil q nur die Teiler $1, q$ hat, von denen der erste von p_1 verschieden ist, nicht anders geschehen kann, als indem p_1 gleich diesem Primfaktor q, etwa $p_1 = q_1$ ist. Hebt man daher diesen gleichen Primfaktor in der Gleichung (21) fort, so findet sich

$$p_2 p_3 \cdots p_\nu = q_2 q_3 \cdots q_\mu$$

und hieraus wieder p_2 gleich einem der Primfaktoren der rechten Seite, etwa $p_2 = q_2$ u. s. f. So zeigt sich allmählich jeder der Primfaktoren p gleich einem der Primfaktoren q, gegen den er sich forthebt; hieraus schliefst man zudem $\mu = \nu$; denn wäre $\mu > \nu$, so würde schliefslich links, wäre $\mu < \nu$, schliefslich rechts die Einheit stehen bleiben, auf der andern Seite mindestens noch ein Primfaktor, durch den sie teilbar sein müfste, was nicht angeht. So ergiebt sich also die völlige Identität der beiden Zerlegungen (19) und (20).

Da, wie schon bemerkt, bei der allmählichen Zerlegung der Zahl m in Primfaktoren ein- und derselbe Primfaktor p wiederholt vorkommen kann, so sollen diese zu Potenzen zusammengefafst gedacht werden. Dann läfst sich das Erreichte in folgendem Hauptsatze von der Teilbarkeit ganzer Zahlen zusammenfassen:

Jede zusammengesetzte (positive) Zahl m kann — und zwar nur in einer ganz bestimmten Weise — als ein Produkt aus Primzahlpotenzen dargestellt werden derart, dafs

$$m = p^a \cdot p_1^{a_1} \cdot p_2^{a_2} \cdots p_{k-1}^{a_{k-1}} \tag{22}$$

gesezt werden darf, wo $p, p_1, p_2, \ldots, p_{k-1}$ verschiedene Primzahlen, $a, a_1, a_2, \ldots, a_{k-1}$ positive ganze Exponenten bedeuten.

Der Fall einer Primzahl $m = p$ ist offenbar als ganz spezieller Fall in diesem allgemeinen Satze enthalten.

6. Die im Vorigen als möglich erkannte Zerlegung einer Zahl m in Primfaktoren wirklich zu ermitteln und so zugleich zu entscheiden, ob m Primzahl sei oder nicht, ist keineswegs einfach, sobald m eine grofse Zahl ist; wir kommen an späterer Stelle auf diese Aufgabe zurück. Die Zwei ist offenbar eine Primzahl und ist die einzige gerade Primzahl, denn alle übrigen geraden Zahlen sind ja Vielfache von 2; mithin sind alle übrigen Primzahlen ungerade Zahlen d. i. von der Form $2z + 1$. Da z sowohl eine gerade Zahl $2x$, als eine ungerade Zahl $2x + 1$ sein kann, sind sie notwendig von einer der beiden Formen $4x + 1$ oder $4x + 3$. Desgleichen sind sie, da z, durch 3 geteilt, nur einen der Reste 0, 1, 2 lassen kann, ausgenommen die Primzahl 3, von einer der Formen $6x + 1$ oder $6x + 5$, deren letztere offenbar dieselben Zahlen liefert, wie die Form $6x - 1$, eben, wie in der Form $4x + 3$ dieselben Zahlen wie in der Form $4x - 1$ enthalten sein werden.

Für nicht zu grofse Zahlen löst man die gedachte Aufgabe durch Versuche, bei denen folgende Bemerkung*), weil sie die Anzahl der erforderlichen Versuche wesentlich einschränkt, von Wichtigkeit ist:

Giebt es bis zur Grenze $\sqrt{m}$**) keine in m aufgehende Primzahl, so ist m selbst eine Primzahl. In der That, wäre m zusammengesetzt und p eine in m aufgehende Primzahl, so müfste diese der Annahme nach gröfser als $\sqrt{m}$ sein. Setzte man demgemäfs

*) S. Legendre, *essai sur la théorie des nombres*, deuxième édition, p. 5. Daselbst findet sich als Tafel IX eine Tabelle der Primzahlen bis 1229. Bei Vega, *tabulae logarithmico-trigonometricae*, Lipsiae 1797, findet man eine solche bis 400 000 reichende Tafel, in der zudem für jede zusammengesetzte Zahl ihr kleinster Primfaktor angegeben ist.

**) Wir müssen hier und gelegentlich auch später in unsere Betrachtungen den Begriff der irrationalen Zahlen übernehmen, ohne auf seine Begründung uns einlassen zu können. Will man ihn hier vermeiden, so setze man statt $\sqrt{m}$ die gröfste ganze Zahl μ, deren Quadrat kleiner als m ist. Bezüglich der Definition und Begründung irrationaler Zahlen mufs auf Werke verwiesen werden, die ihnen besonders gewidmet sind, z. B. auf des Verfassers „*Vorlesungen über die Natur der Irrationalzahlen*, Leipzig 1892“.

$m = pm'$, so würde im Gegenteil m', ebenso wie jeder etwaige Teiler von m' kleiner als $\sqrt{m}$ sein; entweder müſste aber m' selbst oder einer dieser Teiler eine Primzahl sein, die ersichtlich in m aufgeht, und man käme so zu einem Widerspruch gegen die Voraussetzung.

Diese Bemerkung macht es leicht, bis zu einer nicht allzu groſsen Zahl m hin sämtliche Primzahlen zu ermitteln mittels einer Methode, die schon im Altertum unter dem Namen des Siebes von Eratosthenes (*cribrum Eratosthenis*) bekannt war. Man denke sich alle Zahlen bis m hin nach der Reihe aufgestellt, streiche dann in dieser Reihe unter Beibehaltung der Zahl 2 alle Vielfachen von 2; streiche unter den noch übrigen Zahlen der Reihe die darin enthaltenen Vielfachen der nächsten Zahl 3, während man diese Zahl selbst beibehält; dann unter den jetzt noch übrigen Zahlen der Reihe die darin enthaltenen Vielfachen der nächsten Zahl 5 unter Beibehaltung dieser Zahl selbst, u. s. w. Die jedesmal nächste Zahl, die $2, 3, 5, 7, \ldots$, muſs eine Primzahl sein; denn, gilt dies schon für die ihr voraufgehenden Zahlen $2, 3, 5, 7, \ldots$, so gilt es auch für sie selbst, da sie sich nicht unter den Vielfachen jener befunden hat, die doch als die einzigen kleineren Primzahlen ermittelt worden sind, also allein ihre Primfaktoren sein könnten; nun ist aber 2 eine Primzahl, also auch alle die gedachten Zahlen. Hat man jenes Verfahren so fortgesetzt bis zur gröſsten Primzahl p unterhalb der Grenze $\sqrt{m}$, so müssen aus der Reihe $1, 2, 3, \ldots, m$ sämtliche Zahlen fortgefallen sein auſser den in ihr enthaltenen Primzahlen. Denn jede Zahl q der Reihe $1, 2, 3, \ldots, m$, welche von den Zahlen $2, 3, 5, \ldots, p$ verschieden ist, ist entweder ein Vielfaches einer dieser Zahlen also schon gestrichen, oder ist durch keine dieser Primzahlen $< \sqrt{m}$, a fortiori also durch keine der Primzahlen $< \sqrt{q}$ teilbar, mithin eine Primzahl.

7. Schon Euclid (*Elementa*, lib. IX, 20) hat bewiesen, daſs die Menge der Primzahlen unendlich ist. In der That, gäbe es nur eine endliche Menge von Primzahlen, so wäre eine unter ihnen die gröſste (nach Kap. 1, Nr. 7); sie heiſse p. Bildet man dann das Produkt aller vorhandenen Primzahlen und addiert zu demselben die Einheit, so entsteht die Zahl

$$2 \cdot 3 \cdot 5 \cdot 7 \cdots p + 1,$$

welche offenbar $> p$ und durch keine der vorhandenen Primzahlen teilbar, folglich unzerlegbar also noch eine neue Primzahl wäre, gegen die Voraussetzung.

Dies Räsonnement läſst sich nach Kummer (*Berl. Monatsber.* 1878, p. 777) durch das folgende ersetzen. Da, wenn p die gröſste Primzahl wäre, die von 1 verschiedenen Zahlen, welche $< 2 \cdot 3 \cdot 5 \cdot 7 \cdots p$ sind, entweder eine der Primzahlen $2, 3, 5, 7, \ldots, p$ oder doch nur

aus solchen zusammengesetzt sein können, würde jede von ihnen einen Teiler mit $P = 2 \cdot 3 \cdot 5 \cdot 7 \cdots p$ gemeinsam haben, 1 also die einzige Zahl $< P$ sein, welche prim gegen P ist. Aber zwei aufeinanderfolgende Zahlen sind offenbar stets relativ prim; somit wäre $P - 1 > 1$ noch eine zweite zu P prime Zahl $< P$, ein Widerspruch, welcher die Unzulässigkeit der Annahme erweist.

Euler folgerte dasselbe aus einer analytischen Formel, und in seinen Fufstapfen weiterschreitend bewies allgemeiner zuerst P. Lejeune Dirichlet (*Abh. d. Berl. Ak.* 1837, p. 45, *Werke* 1, p. 313), dafs jede arithmetische Progression oder dafs die Formel $mz + n$, in welcher z alle Zahlen der Reihe (Z), die „Differenz“ m aber und „das Anfangsglied“ n zwei relativ prime Zahlen bedeuten, unendlich viel Primzahlen enthalte bezw. darstelle. Diesen ursprünglich von Legendre aufgestellten Satz (*essai sur la th. des nombres* 2, § 9) bewies sodann mit elementareren Hilfsmitteln F. Mertens (*Wiener Berichte* 106, 1897, p. 254, in einer Arbeit, von welcher Teile bereits früher veröffentlicht waren im *Journ. f. Math.* 78, 1874, p. 46 und 117, 1897, p. 169; *Wien. Ber.* 104, 1895, p. 1093, 1159; s. dazu auch ebend. 108 II, Mai 1899), und er vervollständigte den Satz noch durch Angabe von Grenzen, in denen wenigstens eine jener Primzahlen enthalten sein mufs. Für die speziellen arithmetischen Progressionen von der Form $mz + 1$ gab E. Wendt (*Journ. f. Math.* 115, 1895, p. 85) eine rein arithmetische Herleitung des Satzes.

Besondere Fälle dieser Art erledigen sich sehr einfach (s. Lucas, *théorie des nombres*, p. 353). Z. B. schliefst man folgendermafsen, dafs es in der arithmetischen Progression oder in der Form $6x - 1$ unendlich viel Primzahlen giebt. Für jede Primzahl $p > 2$ erhält man durch die Formel

$$2 \cdot 3 \cdot 5 \cdot 7 \cdots p - 1$$

eine Zahl von der Form $6x - 1$. Ist diese, durch 3 nicht teilbare Zahl nicht selbst eine Primzahl, so enthält sie doch mindestens einen Primfaktor von der Form $6x - 1$; denn ein Produkt aus lauter Primfaktoren der anderen, allein noch zulässigen Form $6x + 1$ hat immer wieder die gleiche Form $6x + 1$. Jene Primzahl bezw. ihr eben erwähnter Primfaktor von der Form $6x - 1$ ist aber von jeder der Primzahlen $2, 3, 5, 7, \ldots, p$ verschieden, da der obige Ausdruck durch keine dieser Zahlen aufgeht. Somit kann man, unter p jedesmal die gröfste der bereits ermittelten Primzahlen von der Form $6x - 1$ verstehend, deren kleinste die Primzahl 5 ist, eine noch gröfsere Primzahl derselben Form nachweisen, w. z. b. w.

Wir schliefsen hieran noch folgenden Satz: Die Gleichung

$$(23) \qquad 2 \cdot 3 \cdot 5 \cdot 7 \cdots p = a^m \pm b^m,$$

in welcher $m > 1$ und a, b positive ganze Zahlen bedeuten, ist unmöglich, wenn $p > 2$ ist. Dem Beweise desselben schicken wir den anderen voraus: Der Ausdruck $\alpha^q - \beta^q$, in welchem α, β ganze Zahlen, q eine Primzahl bedeuten, ist entweder prim gegen q oder teilbar durch q^2. (S. hierzu Lucas a. a. O. p. 341, Ex. 4.) Da

$$\frac{\alpha^q - \beta^q}{\alpha - \beta} = \alpha^{q-1} + \alpha^{q-2}\beta + \cdots + \alpha\beta^{q-2} + \beta^{q-1}$$

eine ganze Zahl ist, so ist $\alpha^q - \beta^q$ das Produkt der beiden ganzen Zahlen $\alpha - \beta$, $\frac{\alpha^q - \beta^q}{\alpha - \beta}$, von denen die letztere, wenn $\alpha = \beta + \gamma$ gesetzt wird, in

$$(24) \qquad \frac{\alpha^q - \beta^q}{\alpha - \beta} = q\beta^{q-1} + \frac{q(q-1)}{1 \cdot 2}\beta^{q-2}\gamma + \cdots + q\beta\gamma^{q-2} + \gamma^{q-1}$$

übergeht; mit Rücksicht darauf, dafs die Binomialkoeffizienten der q^{ten} Potenz, wie bald bestätigt werden soll (Ende von Nr. 12), durch q teilbare ganze Zahlen sind, ergiebt dieser Ausdruck, dafs der zweite Faktor $\frac{\alpha^q - \beta^q}{\alpha - \beta}$ zugleich mit dem ersten Faktor $\alpha - \beta = \gamma$ durch q teilbar oder durch q nicht teilbar ist, wie es die voraufgehende Aussage behauptet.

Bestände nun die Gleichung (23), so könnte zunächst keine der Zahlen a, b durch einen der Primfaktoren des Produktes

$$P = 2 \cdot 3 \cdot 5 \cdot 7 \cdots p$$

teilbar sein, denn sonst müfste es auch die andere sein und folglich das Produkt P durch eine höhere als die erste Potenz dieses Primfaktors aufgehen, was nicht der Fall ist. Da aber a, b nicht beide gleich 1 sein können, denn P ist weder Null noch Zwei, so mufs eine dieser Zahlen durch eine gröfsere Primzahl als p teilbar, dieser Primzahl also mindestens gleich und folglich $\overline{\gtrless} p + 2$ sein. — Nun kommt nur der Fall eines ungeraden m in Betracht. Denn für ein gerades $m = 2\mu$ wäre

$$a^m + b^m = (a^\mu)^2 + (b^\mu)^2,$$

da a^μ, b^μ durch 3 nicht teilbare Zahlen sind, deren Quadrate, durch 3 geteilt, stets den Rest 1 geben, nicht durch 3 teilbar, wie es P doch ist;

$$a^m - b^m = (a^\mu)^2 - (b^\mu)^2$$

aber wäre, da a^μ, b^μ ungerade Zahlen sind, deren Quadrate, durch 4 geteilt, stets den Rest 1 geben, durch 4 teilbar, was P nicht ist; weder für das obere noch für das untere Vorzeichen könnte demnach die Gleichung (23) bestehen. Sei somit m ungerade. Dann darf es nicht $> p$ sein, denn für ein solches m wäre $a^m + b^m > (p+2)^p > P$;

damit aber $a^m - b^m = P$ würde, was positiv ist, müfste $a = b + c$, $c \geqq 1$ sein; in diesem Falle würde jedoch

$$a^m - b^m = mb^{m-1}c + \cdots + mbc^{m-1} + c^m,$$

jenachdem $b = 1$ also $a \geqq p + 2$, oder $b > 1$ also $\geqq p + 2$ wäre, gröfser als

$$c^m = (a-1)^m > (p+1)^p$$

oder gröfser als

$$b^{m-1} \geqq (p+2)^p,$$

während P kleiner ist als jeder dieser Werte. Demnach müfste $m \leqq p$ und folglich durch einen der Primfaktoren q von P teilbar sein, die angenommene Gleichung (23) erhielte die Gestalt

$$P = \alpha^q - \beta^q,$$

wo α eine positive, β eine positive oder negative ganze Zahl, q Primzahl ist, wäre aber wieder unmöglich, da nach der voraufgeschickten Bemerkung die rechte Seite den Primfaktor q entweder gar nicht oder mehrfach enthielte, während er in P ein aber auch nur ein Mal auftritt.

8. Hat man der Formel (22) gemäfs eine Zahl m in ihre Primfaktoren zerlegt, so ist es leicht, ihre sämtlichen Teiler aufzustellen. In der That, ist n ein Teiler von m und folglich $m = qn$, so geht offenbar jeder Primteiler von n auch in m auf, also kann n keine anderen Primfaktoren enthalten, als m selbst, und demnach wird seine Zerlegung in Primzahlpotenzen notwendig die Form haben:

$$n = p^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{k-1}^{\alpha_{k-1}}, \tag{25}$$

worin jeder der Exponenten $\alpha, \alpha_1, \ldots$ eine positive ganze Zahl oder, falls die entsprechende Primzahl in n nicht, wie in m selbst, aufgehen sollte, die Null bedeutet. Keiner dieser Exponenten darf aber gröfser sein, als der Exponent derselben Primzahlpotenz in der Zerlegung von m; denn, wäre z. B. $\alpha > a$, so enthielte n den Primfaktor p öfter als a-mal, und er müfste wegen $m = qn$ dann auch in m öfter als a-mal auftreten. Hiernach befinden sich sämtliche Teiler von m unter den Zahlen n von der Form (25), die man erhält, indem man die Exponenten $\alpha, \alpha_1, \ldots, \alpha_{k-1}$ der Reihe nach die Werte

$$\begin{cases} \alpha: & 0, 1, 2, \ldots, a, \\ \alpha_1: & 0, 1, 2, \ldots, a_1, \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \alpha_{k-1}: & 0, 1, 2, \ldots, a_{k-1} \end{cases} \tag{26}$$

durchlaufen läfst. Jede dieser Zahlen ist aber auch ein Teiler von m; denn, bezeichnen $\beta, \beta_1, \ldots, \beta_{k-1}$ die nicht negativen Differenzen

$$a - \alpha,\ a_1 - \alpha_1,\ \cdots,\ a_{k-1} - \alpha_{k-1}$$

resp., so kann man allgemein setzen

$$m = p^{\beta} p_1^{\beta_1} \cdots p_{k-1}^{\beta_{k-1}} \cdot n = qn,$$

wo $q = p^{\beta} p_1^{\beta_1} \cdots p_{k-1}^{\beta_{k-1}}$ eine ganze Zahl ist. Die Gesamtheit der Zahlen n von der Form (25) für die in (26) angegebenen Werte der Exponenten ist also die Gesamtheit der Teiler von m.

Da durch die Kombination aller zulässigen Werte der Exponenten

$$(a+1)(a_1+1) \cdots (a_{k-1}+1)$$

Zahlen von der Form (25) entstehen, so ist die Anzahl $t(m)$ der verschiedenen Teiler von m gleich demselben Produkte:

$$t(m) = (a+1)(a_1+1) \cdots (a_{k-1}+1), \tag{27}$$

und hängt demnach nicht von dem Werte der Primzahlen, aus denen m besteht, sondern nur von ihrer Häufigkeit in der Zerlegung von m ab.

Leicht findet man auch die Summe aller Teiler von m. Wäre m eine Primzahlpotenz, $m = p^a$, so wäre jene Summe ersichtlich die folgende:

$$1 + p + p^2 + \cdots + p^a = \frac{p^{a+1} - 1}{p - 1}.$$

Bildet man aber die analogen, den sämtlichen übrigen Primfaktoren von m entsprechenden Summen:

$$1 + p_1 + p_1^2 + \cdots + p_1^{a_1} = \frac{p_1^{a_1+1} - 1}{p_1 - 1}$$

. . . .

$$1 + p_{k-1} + p_{k-1}^2 + \cdots + p_{k-1}^{a_{k-1}} = \frac{p_{k-1}^{a_{k-1}+1} - 1}{p_{k-1} - 1},$$

so erhält man bei der Multiplikation aller dieser Gleichungen links offenbar als allgemeines Glied den Ausdruck (25) für n, und somit zur Linken der resultierenden Gleichung genau die gesamte Summe dieser Zahlen für die unter (26) angegebenen Werte der Exponenten d. i: die Summe*) $\int(m)$ aller Teiler von m ist:

---

*) Die Bezeichnung der zahlentheoretischen Funktionen ist bisher noch eine bei den verschiedenen Schriftstellern sehr ungleiche. Das Zeichen $\int(m)$ oder $\int m$ für die Summe der Teiler von m stammt von Euler her (*Opusc. var. argum.* 2, 1750, p. 23 = *Comm. arithm.* 1, p. 102); Liouville bedient sich statt dessen des Zeichens $\zeta(m)$ und bezeichnet dem entsprechend mit $\zeta_h(m)$ dasselbe, was hier $\int\limits_h(m)$ genannt ist (*Journ. de Math.*, 2. sér., 2, 1857, p. 425). Tafeln für die Summe der Teiler gab zuerst Euler (s. *Comm. ar.* 1, p. 104—109, 147). Nach Lucas *th. des nombres* p. 378 gaben ihnen Reuschle und Landry (*décomposition des nombres* $2^n \pm 1$, Paris 1869) eine gröſsere Ausdehnung.

(28) $$\int(m) = \frac{p^{\alpha+1}-1}{p-1} \cdot \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdots \frac{p_{k-1}^{\alpha_{k-1}+1}-1}{p_{k-1}-1};$$

diese hängt sowohl von dem Werte der Primfaktoren von m, als auch von der Häufigkeit ihres Auftretens ab.

Betrachtet man an Stelle des Teilers n eine beliebige Potenz n^h desselben, so darf man setzen:

$$n^h = (p^h)^\alpha \cdot (p_1^h)^{\alpha_1} \cdots (p_{k-1}^h)^{\alpha_{k-1}};$$

hiernach leuchtet ein, dafs die Formel (28) die Summe $\int_h(m)$ der h^{ten} Potenzen sämtlicher Teiler von m ergiebt, indem man überall die Primfaktoren durch ihre h^{ten} Potenzen ersetzt, also

(29) $$\int_h(m) = \frac{p^{h(\alpha+1)}-1}{p^h-1} \cdot \frac{p_1^{h(\alpha_1+1)}-1}{p_1^h-1} \cdots \frac{p_{k-1}^{h(\alpha_{k-1}+1)}-1}{p_{k-1}^h-1}.$$

Jedem Teiler n von m entspricht nach der Beziehung $m = qn$ ein anderer q, der zu n komplementäre Teiler, und dieser ist von jenem verschieden, wenn m keine Quadratzahl ist. Im entgegengesetzten Falle, wenn also etwa $m = q^2$ ist, würde dem besonderen Teiler q von m dieser selbe Teiler komplementär sein. Hiernach ist ersichtlich die Anzahl der verschiedenen Teiler von m gerade, etwa 2λ, wenn m keine Quadratzahl, dagegen ungerade, etwa $2\lambda + 1$, wenn m eine Quadratzahl ist. In der That wird m eine solche sein oder nicht, jenachdem in der Zerlegung (22) sämtliche Exponenten a_i gerade sind, oder nicht; im ersteren Falle mufs nach (27) $t(m)$ eine ungerade Zahl sein, im zweiten aber gerade, da dann mindestens einer der Faktoren zur Rechten der Gleichung eine gerade Zahl sein mufs. Nennt man nun zwei Darstellungen $m = qn$, $m = nq$ der Zahl m als Produkt zweier Faktoren nur eine einzige Zerlegung derselben in zwei Faktoren, so ist offenbar die Anzahl dieser Zerlegungen gleich λ oder $\lambda + 1$, jenachdem m keine oder eine Quadratzahl ist, d. i. resp. gleich

(30) $$\frac{1}{2}t(m); \quad \frac{1}{2}\left(t(m)+1\right).$$

Von den Zerlegungen einer Zahl m in zwei Faktoren überhaupt sind diejenigen zu unterscheiden oder herauszuheben, bei denen die zwei Faktoren ohne gemeinsamen Teiler sind. Soll

$$m = p^\alpha p_1^{\alpha_1} \cdots p_{k-1}^{\alpha_{k-1}} = qn$$

und die Faktoren q, n relativ prim sein, so müssen sich die Primteiler von m so auf diese Faktoren verteilen, dafs keine der Primzahlen, die in q aufgehen, auch aufgeht in n; mithin mufs, wenn etwa

p in q aufgeht, zugleich die gesamte Primzahlpotenz p^α auf den Faktor q entfallen u. s. w. Es giebt mithin soviel solcher Darstellungen $m = qn$, als man die Primzahlpotenzen $p^\alpha, p_1^{\alpha_1}, \cdots p_{k-1}^{\alpha_{k-1}}$ oder auch, als man die Primzahlen $p, p_1, \cdots p_{k-1}$ selbst in zwei Gruppen verteilen kann, d. i., da die erste Gruppe $0, 1, 2, \ldots k$ und die zweite dann entsprechend $k, k-1, k-2, \cdots 0$ dieser Zahlen enthalten kann, die Anzahl

$$1 + \frac{k}{1} + \frac{k(k-1)}{1 \cdot 2} + \cdots + \frac{k}{1} + 1$$

oder

$$(1+1)^k = 2^k.$$

Handelt es sich nur um die Anzahl der **Zerlegungen** in zwei relativ prime Faktoren, so ist diese halb so grofs, also 2^{k-1}, da der Fall gleicher Faktoren: $n = q$, bei relativ primen Zerlegungen nicht vorkommen kann. Man ersieht hieraus, dafs diese Anzahl weder von dem Werte der Primfaktoren von m, noch von deren Häufigkeit, sondern einzig von der Anzahl derselben abhängt, sodafs sie die gleiche ist für m, wie für das Produkt $p\, p_1 \ldots p_{k-1}$ seiner Primfaktoren.

9. Sind für mehrere Zahlen $m, m', m'', \ldots$ ihre Zerlegungen in Primfaktoren bekannt, so läfst sich daraus auch ihr gröfster gemeinsamer Teiler sowie ihr kleinstes gemeinsames Vielfache bestimmen. Jeder Teiler aller Zahlen $m, m', m'' \ldots$ kann nämlich, dem oben Gesagten zufolge, nur aus solchen Primfaktoren bestehen, die in jeder der gedachten Zahlen als Faktor enthalten sind; und, wenn p ein solcher Primfaktor ist, so kann die höchste Potenz desselben, welche in jenem Teiler aufgeht, nicht höher sein, als in jeder der Zahlen $m, m', m'', \ldots$ d. i. als die niedrigste Potenz p^γ, welche in deren Zerlegungen auftritt. Man unterdrücke also in diesen Zerlegungen alle Potenzen von Primzahlen, die nicht in ihnen allen enthalten sind, und für die gemeinsam in ihnen enthaltenen bestimme man die niedrigsten darin auftretenden Potenzen; sind diese $p^\gamma, p_1^{\gamma_1}, p_2^{\gamma_2}, \ldots$, so wird jeder gemeinsame Teiler aller Zahlen $m, m', m'', \ldots$ notwendig ein Teiler sein des Produktes

$$\Delta = p^\gamma p_1^{\gamma_1} p_2^{\gamma_2} \ldots . \tag{31}$$

Aber auch umgekehrt wird jeder solcher in allen Zahlen $m, m', m'', \ldots$ aufgehen, da er nur aus solchen Primfaktoren besteht, die in jeder derselben auftreten, und keinen von ihnen öfter enthält, als alle letzteren Zahlen. Unter den so bestimmten gemeinsamen Teilern ist ersichtlich das Produkt Δ der gröfste.

Ein gemeinsames Vielfache aller Zahlen $m, m', m'', \ldots$ enthält, weil durch jede derselben teilbar, die sämtlichen Primzahlen p, welche in ihren Zerlegungen sich finden, und jede derselben in einer min-

destens so hohen Potenz, als sie in irgend einer dieser Zerlegungen auftritt. Man stelle also die sämtlichen, in jenen Zerlegungen vorhandenen Primzahlen auf und bestimme für jede von ihnen die höchste Potenz, die in den gedachten Zerlegungen auftritt; sind diese p^{ε}, $p_1^{\varepsilon_1}$, $p_2^{\varepsilon_2}, \ldots$, so mufs jedes gemeinsame Vielfache der Zahlen $m, m', m'', \ldots$ gewifs durch

$$M = p^{\varepsilon} \cdot p_1^{\varepsilon_1} \cdot p_2^{\varepsilon_2} \ldots \tag{32}$$

teilbar, ein Vielfaches dieser Zahl sein; und umgekehrt ist jedes Vielfache von M, weil es jede der Primzahlpotenzen jeder der Zahlen $m, m', m'', \ldots$ mindestens so hoch enthält, als diese Zahlen resp., durch jede von ihnen teilbar, ein gemeinsames Vielfache der letzteren. Unter all' diesen gemeinsamen Vielfachen ist aber die Zahl M das kleinste.

Sei sie jetzt das kleinste gemeinsame Vielfache zweier Zahlen m, m'. Dem Gesagten zufolge gehen die Potenzen p^{ε}, $p_1^{\varepsilon_1}$, $p_2^{\varepsilon_2}, \ldots$ einzeln entweder in m oder doch in m' auf, möglicherweise auch in beiden. Daher läfst sich M so in zwei relativ prime Faktoren μ, μ' zerlegen, dafs μ in m, μ' in m' aufgeht. In der That braucht man z. B. hierzu nur für μ das Produkt derjenigen jener Primzahlpotenzen zu wählen, die in m aufgehen, für μ' das Produkt der übrigen, welche notwendig dann Teiler von m' sind.

10. Wir wenden nun die Zerlegung in ein Produkt von Primzahlpotenzen auf den besonderen Fall der Faktoriellen d. i. der Ausdrücke von der Form

$$n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n \tag{33}$$

an. Ein solches Produkt kann nur aus Primzahlen bestehen, welche der Reihe $1, 2, 3, \ldots n$ angehören, also $\overline{\gtrless} n$ sind, und es handelt sich darum, für jede solche Primzahl p die höchste Potenz p^{ν} zu finden, die in dem Produkte enthalten ist. Hierbei darf man offenbar von denjenigen Faktoren des letzteren, welche prim gegen p d. i. keine Vielfachen von p sind, völlig absehen und nur die letzteren als Faktoren beibehalten, statt des Produktes (33) also das andere betrachten:

$$1p \cdot 2p \cdot 3p \cdots \left[\frac{n}{p}\right] p = 1 \cdot 2 \cdot 3 \cdots \left[\frac{n}{p}\right] \cdot p^{\left[\frac{n}{p}\right]}.$$

Setzt man zur Abkürzung $\left[\frac{n}{p}\right] = n'$, so darf man hier aus gleichem Grunde statt des Produktes $1 \cdot 2 \cdot 3 \cdots n'$ das andere:

$$1p \cdot 2p \cdot 3p \cdots \left[\frac{n'}{p}\right] p = 1 \cdot 2 \cdot 3 \cdots \left[\frac{n'}{p}\right] \cdot p^{\left[\frac{n'}{p}\right]},$$

mithin statt des Produktes (33) das folgende:

$$1 \cdot 2 \cdot 3 \cdots \left[\frac{n'}{p}\right] \cdot p^{\left[\frac{n}{p}\right] + \left[\frac{n'}{p}\right]}$$

betrachten und nun, wenn zur Abkürzung $\left[\frac{n'}{p}\right] = n''$ gesetzt wird, wieder das folgende:

$$1 \cdot 2 \cdot 3 \cdots \left[\frac{n''}{p}\right] \cdot p^{\left[\frac{n}{p}\right]+\left[\frac{n'}{p}\right]+\left[\frac{n''}{p}\right]}$$

u. s. w. Da die Zahlen $n, n', n'', \ldots$ abnehmende ganze Zahlen sind, wird endlich eine derselben, zuerst etwa die Zahl $n^{(i)}$, kleiner als p und dann dieser Primfaktor im Produkte $1 \cdot 2 \cdot 3 \cdots n^{(i)}$ überhaupt nicht mehr vorhanden sein. Mithin kann man dann für den gedachten Zweck statt des Produktes (33) die Potenz

$$p^{\left[\frac{n}{p}\right]+\left[\frac{n'}{p}\right]+\left[\frac{n''}{p}\right]+\cdots+\left[\frac{n^{(i-1)}}{p}\right]}$$

betrachten, und sie ist folglich die gesuchte höchste Potenz p^ν, die in der Faktorielle $1 \cdot 2 \cdot 3 \cdots n$ aufgeht. Der Exponent ν derselben bestimmt sich also durch die Formel:

$$\nu = \left[\frac{n}{p}\right] + \left[\frac{n'}{p}\right] + \left[\frac{n''}{p}\right] + \cdots + \left[\frac{n^{(i-1)}}{p}\right]. \tag{34}$$

Ist z. B. $n = 1900$ und $p = 2$, so findet sich allmählich

$$\begin{aligned}
n' &= \left[\frac{1900}{2}\right] = 950 \\
n'' &= \left[\frac{950}{2}\right] = 475 \\
n''' &= \left[\frac{475}{2}\right] = 237 \\
n^{(4)} &= \left[\frac{237}{2}\right] = 118 \\
n^{(5)} &= \left[\frac{118}{2}\right] = 59 \\
n^{(6)} &= \left[\frac{59}{2}\right] = 29 \\
n^{(7)} &= \left[\frac{29}{2}\right] = 14 \\
n^{(8)} &= \left[\frac{14}{2}\right] = 7 \\
n^{(9)} &= \left[\frac{7}{2}\right] = 3 \\
n^{(10)} &= \left[\frac{3}{2}\right] = 1
\end{aligned}$$

und durch Addition dieser Werte $\nu = 1893$, d. i. 2^{1893} ist die höchste Potenz von 2, die im Produkte aller Zahlen von 1 bis 1900 als Faktor enthalten ist.

Die Formel (34) läſst sich jedoch durch eine bequemere ersetzen, in welcher man der abgeleiteten Zahlen $n', n'', \ldots n^{(i-1)}$ nicht bedarf.

Hierzu dient die allgemeine Bemerkung, dafs, wenn n' die gröfste in $\frac{n}{a}$, n'' die gröfste in $\frac{n'}{b}$ enthaltene ganze Zahl ist, n'' zugleich das gröfste in $\frac{n}{ab}$ enthaltene Ganze ist. In der That, ist $\frac{n}{a} = n' + \frac{r}{a}$, wo $0 \overline{\overline{<}} r < a$ ist, so folgt $\frac{n}{ab} = \frac{n'}{b} + \frac{r}{ab}$; sei nun $\frac{n'}{b} = n'' + \frac{s}{b}$, wo $0 \overline{\overline{<}} s < b$ ist, so wird

$$\frac{n}{ab} = n'' + \frac{as + r}{ab},$$

wo $as + r$ höchstens gleich $a(b-1) + a - 1 = ab - 1$ also $0 \overline{\overline{<}} as + r < ab$ und folglich $n'' = \left[\frac{n}{ab}\right]$ ist, w. z. b. w. — Indem man nun a successive gleich $p, p^2, p^3, \ldots$; b aber gleich p wählt, findet man hiernach

$$n' = \left[\frac{n}{p}\right], \quad n'' = \left[\frac{n'}{p}\right] = \left[\frac{n}{p^2}\right], \quad n''' = \left[\frac{n''}{p}\right] = \left[\frac{n}{p^3}\right], \quad \cdots$$

und demnach statt der Formel (34) diese neue Bestimmung:

$$(35) \qquad \nu = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots,$$

welche soweit fortgesetzt werden mufs, als die Potenz von p im Nenner der Symbole noch kleiner als n ist, welche unbedenklich aber auch durch die nachstehende ersetzt werden darf:

$$(36) \qquad \nu = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right],$$

da das allgemeine Glied dieser Reihe von selbst verschwindet, sobald die Potenz von p im Nenner die Zahl n übertrifft.

11. Die so umgestaltete Formel ist besonders bequem unter der Voraussetzung, dafs man zuvor die Zahl n in eine Form gesetzt habe, in welche sie stets auf eindeutig bestimmte Weise gebracht werden kann.

Sei zunächst p allgemein irgend eine positive ganze Zahl. Da die successiven Potenzen derselben allmählich über die Grenze n aufsteigen werden, so giebt es eine bestimmte dieser Potenzen, p^h, welche noch kleiner oder doch wenigstens nicht gröfser als n ist, während p^{h+1} schon n übertrifft, d. h., für welche

$$p^h \overline{\overline{<}} n < p^{h+1}$$

ist. Schaltet man demnach zwischen diese beiden Potenzen die Werte ein:

$$2p^h, \; 3p^h, \cdots (p-1)p^h,$$

so muss wieder n, wenn nicht an der Grenze eines der Teilintervalle, so innerhalb eines derselben liegen, sodafs man, unter a eine der Zahlen $1, 2, 3, \ldots p-1$ verstehend,

$$ap^h \overline{\gtrless} n < (a+1)p^h$$

mithin $n = ap^h + n'$ setzen darf, wo $0 \overline{\gtrless} n' < p^h$ ist. Indem man bezüglich n' verfährt, wie soeben mit Bezug auf n, findet sich $n' = bp^k + n''$, wo $k < h$ und $0 \overline{\gtrless} n'' < p^k$ ist, u. s. w. So findet sich dann

$$n = ap^h + bp^k + cp^l + \cdots,$$

wo die Koeffizienten sämtlich positive ganze Zahlen $< p$, die Exponenten $h, k, l, \ldots$ eine abnehmende Reihe positiver ganzer Zahlen vorstellen. Statt dessen darf man offenbar, indem man für die Koeffizienten noch den Wert 0 zuläſst, auch schreiben:

$$n = ap^h + a_1 p^{h-1} + a_2 p^{h-2} + \cdots + a_{h-1} p + a_h. \tag{37}$$

Diese Darstellung einer Zahl*) n auf Grund einer anderen gegebenen Zahl p (mittels der Grundzahl oder der Basis p) verwandelt sich für den besonderen Fall $p = 10$ in die gewohnte dekadische Schreibweise einer Zahl, bei welcher die Basis 10 ist; denn z. B. ist die Zahl 120759 nichts anderes als:

$$1 \cdot 10^5 + 2 \cdot 10^4 + 0 \cdot 10^3 + 7 \cdot 10^2 + 5 \cdot 10^1 + 9;$$

die Koeffizienten der Darstellung sind die Ziffern der dargestellten Zahl. Bei Zugrundelegung der Basis $p = 7$ dagegen würde dieselbe Zahl gleich

$$1 \cdot 7^6 + 0 \cdot 7^5 + 1 \cdot 7^4 + 2 \cdot 7^3 + 0 \cdot 7^2 + 3 \cdot 7^1 + 2,$$

in den dieser Darstellung entsprechenden Ziffern also zu schreiben sein:

$$1012032,$$

was man andeutet durch die Beziehung

$$(1012032)_7 = (120759)_{10}.$$

So entspricht jeder anderen Grundzahl wieder ein anderes Ziffernsystem der betrachteten Zahl, und es ist von Interesse, zu untersuchen, in welcher Weise sich die Folge der Ziffern verändert, wenn man von einer Grundzahl zu einer anderen übergeht, oder wie die der einen entsprechende Folge aus der zur anderen gehörigen gefunden werden kann; es leuchtet z. B. an sich ein, daſs jede wesentliche Eigenschaft der dargestellten Zahl d. i. eine Eigenschaft derselben, die von der besonderen Wahl der Grundzahl unabhängig ist, zu einer bestimmten „invarianten“ Eigenschaft ihres Ziffernsystems Anlaſs geben muſs, welche aufzuspüren sein würde. J. Kraus hat in einer gröſseren Arbeit (*Zeitschr. f. Math. u. Phys.* 37, 1892, p. 321 und 39, 1894, p. 11) den Anfang dazu gemacht, diesen gesetzmäſsigen

---

*) Sie ist nur ein spezieller Fall der Darstellung einer Zahl „in einfachen Zahlensystemen“, wie sie von G. Cantor „über die einfachen Zahlensysteme“, *Ztschr. f. Math. u. Phys.* 14, 1869, p. 121 angegeben worden ist.

Zusammenhang zu untersuchen; an späterer Stelle (Kap. 7 nr. 16) kommen wir auf zwei bezügliche, von ihm abgeleitete Sätze zurück; hier sollen nur noch zwei sehr einfache besondere Fälle der Darstellung (37) hervorgehoben werden.

Für $p = 2$ können „die Ziffern" a_i in (37) nur einen der Werte 0 oder 1 haben, und es ergiebt sich daher sogleich der Satz: Jede positive ganze Zahl, welche kleiner ist als 2^{h+1}, läfst sich in eindeutiger Weise als Summe **verschiedener** der niedrigeren Potenzen $2^h, 2^{h-1}, \ldots 2, 1$ darstellen. Die Summe der Ziffern: $a + a_1 + a_2 + \cdots + a_h$ ist in diesem Falle offenbar nichts anderes als die zu jener Darstellung erforderliche Anzahl der genannten Potenzen.

Für $p = 3$ erhielte man

$$n = a \cdot 3^h + a_1 \cdot 3^{h-1} + \cdots + a_{h-1} \cdot 3 + a_h,$$

wo die Koeffizienten nur einen der Werte 0, 1, 2 haben können. Jedes Glied von der Gestalt $2 \cdot 3^i$ kann durch $3^{i+1} - 1 \cdot 3^i$ ersetzt werden; indem man diese Umformung vom letzten Gliede an überall, wo es zutrifft, ausführt, kann der voraufgehende Koeffizient, wenn er 1 war, 2 werden und zu einer neuen Umformung Anlafs geben, oder, wenn er schon 2 war, 3 werden, wo dann die Potenz von 3 sich um eine Einheit erhöht und zur voraufgehenden zu ziehen ist. Auf solche Weise kann es geschehen, dafs noch die Potenz 3^{h+1} eingeführt wird. Da dann aber sämtliche Koeffizienten einen der Werte 0, 1, -1 haben, geht der Satz hervor: Jede positive ganze Zahl $\lesseqgtr 3^{h+1}$ kann als Aggregat **verschiedener** der Potenzen $3^{h+1}, 3^h, 3^{h-1}, \ldots 3, 1$ dargestellt, d. h. aus solchen durch Additionen und Subtraktionen gebildet werden.

Kehren wir nun zu dem Falle zurück, in welchem p eine Primzahl bedeutet, so läfst sich die Formel (35) vermittelst der Darstellung (37) sehr einfach gestalten. Aus (37) folgen nämlich nachstehende Gleichungen:

$$(38)\quad \begin{cases} \left[\frac{n}{p}\right] = ap^{h-1} + a_1 p^{h-2} + \cdots + a_{h-2} p + a_{h-1} \\ \left[\frac{n}{p^2}\right] = ap^{h-2} + a_1 p^{h-3} + \cdots + a_{h-2} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \left[\frac{n}{p^{h-1}}\right] = ap + a_1 \\ \left[\frac{n}{p^h}\right] = a \end{cases}$$

und nun verschwinden sämtliche folgenden Ausdrücke $\left[\frac{n}{p^{h+1}}\right], \left[\frac{n}{p^{h+2}}\right], \cdots$ Demgemäfs erhält man ν durch Addition der Gleichungen (38), nämlich

$$\nu = a \cdot \frac{p^h - 1}{p - 1} + a_1 \cdot \frac{p^{h-1} - 1}{p - 1} + \cdots + a_{h-2} \cdot \frac{p^2 - 1}{p - 1} + a_{h-1} \cdot \frac{p - 1}{p - 1}$$

oder

(39) $$\nu = \frac{n - (a + a_1 + \cdots + a_{h-1} + a_h)}{p - 1}.$$

(S. hierzu Legendre, *essai sur la th. des nombres*, 2. édit. p. 10.) Z. B. folgt aus der Darstellung der Zahl 120759 im Zahlensysteme mit der Grundzahl 7:

$$\nu = \frac{120759 - 9}{6} = 20125$$

als Exponent der höchsten im Produkte der Zahlen von 1 bis 120759 aufgehenden Potenz von 7.

Besonders einfach wird die Legendresche Formel für den Fall $p = 2$. Heifst dann k die Anzahl verschiedener Potenzen von 2, durch deren Addition n entsteht, so ist

$$\nu = n - k$$

der Exponent der höchsten in $1 \cdot 2 \cdot 3 \cdots n$ aufgehenden Potenz von 2. Z. B. ist

$$n = 1900 = 2^{10} + 2^9 + 2^8 + 2^6 + 2^5 + 2^3 + 2^2,$$

$k = 7$, $\nu = 1893$, wie in Nr. 10 auf andere Weise gefunden worden ist.*)

12. Von diesen allgemeinen Formeln sollen nun ein paar interessante Anwendungen gemacht werden.

Nach dem polynomischen Lehrsatze ist

$$(x + y + z + \cdots)^m = \sum C^m_{q,r,s,\ldots} \cdot x^q y^r z^s \ldots,$$

wo

(40) $$C^m_{q,r,s,\ldots} = \frac{m!}{q!\, r!\, s! \ldots}$$

gesetzt und über alle nicht negativen ganzzahligen Werte von $q, r, s, \ldots$ summiert werden mufs, deren Summe

(41) $$q + r + s + \cdots = m$$

ist. Aus dieser Entstehungsweise des Polynomialkoeffizienten $C^m_{q,r,s,\ldots}$ geht hervor, dafs er einen ganzzahligen Wert hat; man kann dies aber für seinen Ausdruck (40) auch rein arithmetisch mittels der Formel von Legendre bestätigen. Es leuchtet unmittelbar ein für die Koeffizienten der Potenzen x^m, y^m, z^m, ... d. h., wenn die Zahlen $q, r, s, \ldots$ bis auf eine gleich 0 sind, denn dann ist die übrige gleich m, also $C^m_{q,r,s,\ldots}$ gleich 1. Um es auch für die übrigen Koeffizienten zu zeigen, sei p irgend eine Primzahl; diese geht in den

*) S. hierzu Kap. 5, Ende.

verschiedenen Faktoriellen des Ausdrucks (40) genau so oft auf, als nachstehende Summen angeben: im Zähler

$$\left[\frac{m}{p}\right]+\left[\frac{m}{p^2}\right]+\left[\frac{m}{p^3}\right]+\cdots \text{ mal}; \tag{42}$$

in den Faktoren des Nenners resp.

$$\begin{cases} \left[\frac{q}{p}\right]+\left[\frac{q}{p^2}\right]+\left[\frac{q}{p^3}\right]+\cdots \\ \left[\frac{r}{p}\right]+\left[\frac{r}{p^2}\right]+\left[\frac{r}{p^3}\right]+\cdots \\ \left[\frac{s}{p}\right]+\left[\frac{s}{p^2}\right]+\left[\frac{s}{p^3}\right]+\cdots \\ \cdots\cdots\cdots\cdots \end{cases} \tag{43}$$

mal. Aber aus (41) schliefst man

$$\left[\frac{m}{p^i}\right] \overline{\gtrless} \left[\frac{q}{p^i}\right]+\left[\frac{r}{p^i}\right]+\left[\frac{s}{p^i}\right]+\cdots,$$

sodafs jede der in (43) stehenden Kolonnen nicht gröfser ist, als der entsprechende Summande in (42) und demnach die Primzahl p sich aus dem Nenner gegen den Zähler fortheben mufs. Demgemäfs ist der gesamte Bruch (40) eine ganze Zahl. Diese ganze Zahl ist zudem ein Vielfaches von p, wenn m eine Primzahl p ist. Denn in diesem Falle ist der Nenner N von (40), weil aus lauter Faktoren zusammengesetzt, welche kleiner als p, also prim zu p sind, selbst prim gegen p; da nun der Zähler ein Vielfaches von p, gleich $p \cdot M$ ist und durch N aufgeht, mufs M durch N aufgehen, mithin der Bruch (40) gleich $p \cdot \frac{M}{N}$ d. i. ein Vielfaches von p sein.

Insbesondere ist hiernach auch der Binomialkoeffizient, nämlich der Ausdruck

$$\frac{m!}{q!\,r!} = \frac{1 \cdot 2 \cdot 3 \cdots (q+r)}{1 \cdot 2 \cdots q \cdot 1 \cdot 2 \cdots r}$$

eine ganze Zahl. Da man ihn auch folgendermafsen schreiben kann:

$$\frac{(q+1)(q+2)\cdots(q+r)}{1 \cdot 2 \cdots r},$$

so erkennt man, dafs das Produkt von r aufeinanderfolgenden Zahlen stets durch dasjenige der ersten r Zahlen teilbar ist. Ist m eine Primzahl p, so sind dem Zusatze zufolge die Binomialkoeffizienten Vielfache von p; sonach findet man: In der Binomialentwicklung

$$(x+y)^p = x^p + \frac{p}{1}x^{p-1}y + \frac{p(p-1)}{1 \cdot 2}x^{p-2}y^2 + \cdots + \frac{p(p-1)}{1 \cdot 2}x^2y^{p-2} + \frac{p}{1}xy^{p-1} + y^p$$

sind sämtliche Koeffizienten, mit Ausnahme des ersten und

letzten, durch p teilbare ganze Zahlen, sobald p eine Primzahl ist.

13. Setzt man die Summanden in (41), deren Anzahl n sei, einander gleich voraus, sodafs $m = nq$ wird, so ergiebt sich der Bruch $\frac{(nq)!}{(q!)^n}$ als eine ganze Zahl. Dies folgt auch daraus, dafs wegen $nq = (n-1)\,q + q$ der Binomialkoeffizient

$$(44) \qquad \frac{(nq)!}{((n-1)\,q)!\; q!}$$

eine ganze Zahl sein mufs. Nimmt man nämlich als bereits feststehend an, dafs $\frac{((n-1)\,q)!}{(q!)^{n-1}}$ eine ganze Zahl Q sei, so läfst sich dieser Binomialkoeffizient durch

$$\frac{(nq)!}{Q \cdot (q!)^n}$$

ersetzen und lehrt, dafs umsomehr auch $\frac{(nq)!}{(q!)^n}$ ganzzahlig ist; für $n = 1$ leuchtet die Behauptung aber von selber ein. Hierzu hat nun M. Weill (*C. R. de l'Ac. de Paris* 93, 1881, p. 1066) die wertvolle Bemerkung gemacht, dafs der ganzzahlige Wert des Quotienten $\frac{(nq)!}{(q!)^n}$ sogar noch durch $n!$ teilbar, mit anderen Worten, dafs

$$(45) \qquad \frac{(nq)!}{n!\,(q!)^n}$$

eine ganze Zahl sei, und zwar hat er diesen Satz mittels kombinatorischer Betrachtungen bewiesen. Sehr einfach zeigt man ihn rein arithmetisch auf folgende Weise (s. C. de Polignac, *C. R.* 96, 1883, p. 485). Der Quotient (44) findet sich gleich

$$\frac{((n-1)\,q+1)\,((n-1)\,q+2)\cdots((n-1)\,q+q-1)}{1 \cdot 2 \cdot \cdots (q-1)} \cdot n,$$

wo der erste Bruchfaktor einem kurz voraufgehenden Satze zufolge eine ganze Zahl ist, die wir mit q_n bezeichnen wollen. Somit darf man setzen:

$$(nq)! = ((n-1)\,q)!\; 1 \cdot 2 \cdot 3 \cdots q \cdot nq_n;$$

ebenso aber auch

$$((n-1)\,q)! = ((n-2)\,q)!\; 1 \cdot 2 \cdot 3 \cdots q \cdot (n-1)\,q_{n-1}$$

u. s. w., bis

$$(2q)! = (1q)!\; 1 \cdot 2 \cdot 3 \cdots q \cdot 2q_2,$$

Gleichungen, denen man noch die folgende:

$$(1q)! = 1 \cdot 2 \cdot 3 \cdots q \cdot 1q_1,$$

für $q_1 = 1$ hinzufügen kann. Durch ihre Multiplikation miteinander geht aber die andere:

$$(nq)! = (1 \cdot 2 \cdot 3 \cdots q)^n \cdot 1 \cdot 2 \cdot 3 \cdots n \cdot q_1 q_2 \cdots q_n$$

oder:

$$\frac{(nq)!}{n!\,(q!)^n} = q_1 q_2 q_3 \cdots q_n$$

hervor, und so hat man nicht nur den Weillschen Satz, dafs der Quotient (45) eine ganze Zahl sei, bewiesen, sondern auch den ganzzahligen Wert des Quotienten bestimmt.

D. André (*C. R.* 94, 1881, p. 426) ist noch einen Schritt weiter gegangen, indem er den Weillschen Satz als Spezialfall eines anderen nachwies, aus welchem dann hervorgeht, dafs der Bruch $\frac{(nq)!}{(q!)^n}$ nicht nur durch $n!$, sondern sogar durch eine gewisse Potenz dieser Faktoriellen teilbar ist. Der Satz von André lautet folgendermafsen: Ist es nicht möglich, die Zahl q als Summe von weniger denn k Potenzen irgend einer Primzahl darzustellen, beträgt — mit anderen Worten — die Ziffernsumme der Zahl q in jedem Zahlensysteme, dessen Grundzahl eine Primzahl ist, mindestens k, so ist der Bruch $\frac{(nq)!}{(q!)^n}$ teilbar durch $(n!)^k$. Da k für jede Zahl $q > 1$ mindestens 1 ist, folgt hieraus ersichtlich der Weillsche Satz.

Um jene Aussage zu beweisen, sei p irgend eine Primzahl und z die Anzahl, wie oft sie in dem reduzierten Werte des gedachten Bruches vorhanden ist; mit $P(m)$ bezeichnen wir, wie oft sie in der Faktoriellen $m!$ als Faktor enthalten ist. Dann ist

$$z = P(nq) - n \cdot P(q). \tag{46}$$

Nehmen wir zunächst an, q habe im Zahlensysteme mit der Grundzahl p die Gestalt

$$q = \gamma p^2 + \beta p + \alpha.$$

Da

$$\frac{(nq)!}{(n\alpha)!\,(n\beta p)!\,(n\gamma p^2)!}$$

eine ganze Zahl ist, ergiebt sich

$$P(nq) \overline{\gtrless} P(n\alpha) + P(n\beta p) + P(n\gamma p^2),$$

und da $(n\beta p)!$ durch $(n\beta)!\,p^{n\beta}$, ebenso $(n\gamma p^2)!$ durch $(n\gamma p)!\,p^{n\gamma p}$ und dies wieder durch $(n\gamma)!\,p^{n\gamma + n\gamma p}$ aufgeht, so erschliefst man umsomehr

$$P(nq) \overline{\gtrless} P(n\alpha) + n\beta + P(n\beta) + n\gamma + n\gamma p + P(n\gamma),$$

während

$$P(q) = \gamma + \gamma p + \beta$$

ist. Sonach wird

$$z \overline{\gtrless} P(n\alpha) + P(n\beta) + P(n\gamma)$$

und umsomehr

$$z \overline{\gtrless} (\alpha + \beta + \gamma) \cdot P(n).$$

Ganz auf dieselbe Weise fände man aber, falls allgemeiner

$$q = \alpha + \beta p + \gamma p^2 + \delta p^3 + \cdots$$

wäre,

$$z \overline{\gtrless} (\alpha + \beta + \gamma + \delta + \cdots) \cdot P(n).$$

Nach der Annahme ist nun die Ziffernsumme $\alpha + \beta + \gamma + \delta + \cdots \overline{\gtrless} k$, folglich findet sich

$$z \overline{\gtrless} k \cdot P(n)$$

d. h. p geht in dem in Frage stehenden reduzierten Bruche mindestens k-mal so oft auf, wie in der Faktoriellen $n!$, oder mindestens so oft wie in $(n!)^k$. Da dies für jede beliebige Primzahl p gilt, so ist jener Bruch, wie behauptet, teilbar durch $(n!)^k$.

Man kann aber die höchste Potenz der Faktoriellen $n!$, welche in jenem Bruche aufgeht, noch genauer präzisieren (s. de Polignac a. a. O). Dazu bedürfen wir zweier Sätze, die auch sonst ihrer Natur nach hierher gezogen werden dürfen. Sei p eine beliebig gewählte Grundzahl, q, n zwei positive ganze Zahlen. Wenn sie im Zahlensysteme mit der Grundzahl p dargestellt werden, darf man annehmen, dafs sie aus gleich viel Stellen bestehen, indem man erforderlichen Falles der einen von ihnen am Anfange eine oder mehrere Stellen mit der Ziffer 0 hinzufügt. Wir setzen mithin

$$(47) \qquad \begin{cases} q = \mu p^h + \mu_1 p^{h-1} + \cdots + \mu_h \\ n = \nu p^h + \nu_1 p^{h-1} + \cdots + \nu_h; \end{cases}$$

hierbei sind die sämtlichen Ziffern μ_i, ν_i nicht negative ganze Zahlen $< p$. Bildet man nun die Summe $q + n$, so wird $\mu_h + \nu_h < 2p$ sein, mithin

$$(48) \qquad \mu_h + \nu_h = \delta_h p + \sigma_h$$

gesetzt werden können, während δ_h die Null oder Eins, σ_h eine nicht negative Zahl $< p$ bedeutet, sodafs auch $\mu_{h-1} + \nu_{h-1} + \delta_h \overline{\lessgtr} 2(p-1) + 1$ d. i. $< 2p$ sein mufs, mithin wieder

$$(48) \qquad \mu_{h-1} + \nu_{h-1} + \delta_h = \delta_{h-1} p + \sigma_{h-1}$$

gesetzt werden kann, wo δ_{h-1} gleich 0 oder 1, σ_{h-1} nicht negativ und $< p$ ist, u. s. w. Setzen wir demgemäfs bei analoger Bedeutung der Zeichen δ_i, σ_i

$$(48) \qquad \begin{cases} \mu_{h-2} + \nu_{h-2} + \delta_{h-1} = \delta_{h-2} p + \sigma_{h-2} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \mu_1 \quad + \nu_1 \quad + \delta_2 \quad = \delta_1 p \quad + \sigma_1 \\ \mu \quad + \nu \quad + \delta_1 \quad = \delta p \quad + \sigma. \end{cases}$$

Durch Multiplikation sämtlicher Gleichungen (48) mit $1, p, p^2, \ldots p^h$ resp. und nachfolgende Addition ergiebt sich zunächst:

$$(49) \qquad q + n = \delta p^{h+1} + \sigma p^h + \sigma_1 p^{h-1} + \cdots \sigma_h,$$

andererseits liefern jene Gleichungen durch unmittelbare Addition die Beziehung

$$(50)\qquad \begin{aligned}&(\mu + \mu_1 + \cdots + \mu_h) + (\nu + \nu_1 + \cdots + \nu_h)\\ &= (\delta + \sigma + \sigma_1 + \cdots + \sigma_h) + (p-1)(\delta + \delta_1 + \delta_2 + \cdots + \delta_h).\end{aligned}$$

Offenbar bezeichnet $\delta + \delta_1 + \delta_2 + \cdots + \delta_h$ die Anzahl der Einheiten, welche man bei der Addition der beiden Zahlen q, n von einer Stelle auf die nächst höhere übertragen mufs. Daher spricht den Formeln (47) und (49) gemäfs die voraufgehende Beziehung den folgenden Satz aus: Die Summe aus den Ziffern zweier Zahlen q, n übertrifft die Ziffernsumme von $q+n$ um das Produkt aus der um 1 verminderten Grundzahl in die Anzahl der Einheiten, die bei der Addition zu übertragen sind.

Es leuchtet sofort ein, dafs dieser Satz auch für eine Summe mehrerer Zahlen unverändert bestehen bleibt.

Ein ähnlicher Satz gilt aber auch für die Multiplikation. Zur Bildung des Produktes qn denken wir q nach der ersten der Formeln (47) mit $\nu_i p^{h-i}$ multipliziert. Da die Koeffizienten $\mu_i, \nu_i < p$ sind, wird $\mu_h \nu_i < p^2$ sein und also darf

$$(51)\qquad \mu_h \nu_i = \delta_h^{(i)} \cdot p + \pi_h^{(i)}, \quad \text{wo} \quad \delta_h^{(i)}, \pi_h^{(i)} < p \text{ sind,}$$

gesetzt werden. Nunmehr wird $\mu_{h-1}\nu_i + \delta_h^{(i)} \overline{\gtrless} (p-1)^2 + p - 1 < p^2$ sein; man darf also ähnlich wieder setzen:

$$(51)\qquad \mu_{h-1}\nu_i + \delta_h^{(i)} = \delta_{h-1}^{(i)} p + \pi_{h-1}^{(i)}$$

u. s. w., also

$$(51)\qquad \begin{cases} \mu_{h-2}\nu_i + \delta_{h-1}^{(i)} = \delta_{h-2}^{(i)} p + \pi_{h-2}^{(i)} \\ \cdots\cdots\cdots\cdots \\ \mu_1 \nu_i + \delta_2^{(i)} = \delta_1^{(i)} p + \pi_1^{(i)} \\ \mu \nu_i + \delta_1^{(i)} = \delta^{(i)} p + \pi^{(i)}. \end{cases}$$

Durch Multiplikation der sämtlichen Gleichungen (51) mit p^{h-i}, $p^{h-i+1}, \ldots p^{2h-i}$ resp. und nachfolgende Addition gewinnt man zunächst das Ergebnis:

$$(52)\qquad q \cdot \nu_i p^{h-i} = \delta^{(i)} p^{2h-i+1} + \pi^{(i)} p^{2h-i} + \cdots + \pi_{h-1}^{(i)} p^{h-i+1} + \pi_h^{(i)} p^{h-i},$$

während unmittelbar durch ihre Addition sich die Beziehung ergiebt:

$$(53)\qquad \begin{aligned}&(\mu + \mu_1 + \cdots + \mu_h)\nu_i\\ &= (\delta^{(i)} + \pi^{(i)} + \cdots + \pi_h^{(i)}) + (p-1)(\delta^{(i)} + \delta_1^{(i)} + \cdots + \delta_h^{(i)}),\end{aligned}$$

in welcher die erste Klammer rechts die Ziffernsumme der Zahl $q \cdot \nu_i p^{h-i}$, die letzte Klammer dagegen die Anzahl der Einheiten bedeutet, welche bei Ausführung dieser partiellen Multiplikation übertragen werden müssen. Denkt man sich aber die Formel (52) für alle Werte $i = 0, 1, 2, \ldots h$ gebildet d. h. sämtliche partielle Multi-

plikationen ausgeführt, so giebt die Addition dieser Formeln das Produkt qn; die Addition der entsprechenden Gleichungen (53) aber lehrt, dafs das Produkt der Ziffernsummen von q und von n die aus den Ziffernsummen der Zahlen $q \cdot v_i p^{h-i}$ gebildete Summe um die $(p-1)$-malige Anzahl aller bei den einzelnen Multiplikationen zu übertragenden Einheiten übertrifft. Da nun nach dem voraufgehenden Summensatze jene Summe wieder die Ziffernsumme des Produktes qn um die $(p-1)$-malige Anzahl der bei der gedachten Addition der Teilprodukte zu übertragenden Einheiten übertrifft, so findet sich insgesamt folgender zweite Satz: Das Produkt aus den Ziffernsummen zweier Zahlen q, n übertrifft die Ziffernsumme des Produktes qn um den Wert des Produktes aus der um 1 verminderten Grundzahl in die Anzahl aller bei der Bildung der einzelnen Teilprodukte sowie bei deren Addition zu übertragenden Einheiten. Heifst $S(q)$ die Summe der Ziffern der Zahl q, E die gedachte Anzahl der zu übertragenden Einheiten, so ist mithin

$$S(q) \cdot S(n) = S(qn) + (p-1)E. \tag{54}$$

Z. B. handele es sich um das Produkt der im dekadischen Systeme dargestellten Zahlen 7053, 234; hier ist das Schema der Multiplikation, durch welche es gebildet wird, das nachstehende:

$$\begin{array}{ccccccc}
 & & & 7 & 0 & 5 & 3 \\
 & & & & 2 & 3 & 4 \\
\hline
 & & \underline{2} & 8 & \underline{2} & \underline{1} & 2 \\
 & \underline{2} & 1 & \underline{1} & 5 & 9 & \\
\underline{1} & 4 & \underline{1} & 0 & 6 & & \\
 & & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & & \\
\hline
1 & 6 & 5 & 0 & 4 & 0 & 2\,.
\end{array}$$

Die unterstrichenen Zahlen sind die bei den Multiplikationen, die untergesetzten Einheiten die bei der Addition übertragenen Einheiten; man findet aber in der That:

$$(7+0+5+3)(2+3+4) = (1+6+5+0+4+0+2) + 9 \cdot 13.$$

Kehren wir von diesen beiden Hilfssätzen zur Untersuchung des Bruches $\frac{(nq)!}{(q!)^n}$ wieder zurück. Nach der Legendreschen Formel (39) tritt ein Primfaktor p in diesem Quotienten so oft auf, als der folgende Ausdruck:

$$\frac{nq - S(nq)}{p-1} - n \cdot \frac{q - S(q)}{p-1} = \frac{nS(q) - S(nq)}{p-1}$$

angiebt, während er

$$\nu = \frac{n - S(n)}{p-1}$$

mal in $n!$ enthalten ist. Demnach findet man ihn im Quotienten

(55) $$\frac{(nq)!}{(n!)^{\lambda}\cdot(q!)^n},$$

in welchem λ eine positive ganze Zahl bedeute,

$$\frac{nS(q)-S(nq)}{p-1}-\lambda\nu$$

mal, eine Anzahl, welche nach (54) gleich $(S(q)-\lambda)\nu+E$, oder, wenn

$$E=\nu\varepsilon+\varrho, \quad 0 \overline{\overline{<}} \varrho < \nu$$

gesetzt wird, gleich

(56) $$(S(q)+\varepsilon-\lambda)\nu+\varrho$$

ist. Wählt man demnach $\lambda > S(q)+\varepsilon$, so kann der Quotient (55) nicht mehr ganzzahlig sein, da dann der Ausdruck (56) negativ wird; dagegen fällt dieser für $\lambda \overline{\overline{<}} S(q)+\varepsilon$ noch nicht negativ aus. Um daher die höchste Potenz von $n!$ zu finden, welche im Bruche $\frac{(nq)!}{(q!)^n}$ aufgeht, bilde man für alle Primzahlen p, welche $\overline{\overline{<}}\, n$ sind, den Ausdruck $S(q)+\varepsilon$; ist λ unter den so gefundenen Werten der kleinste, so ist $(n!)^{\lambda}$ die gesuchte höchste Potenz.

Z. B. findet sich, wenn $n=5$, $q=12$ also $nq=60$ ist,

für $p=2$: $\quad 5=1\cdot 2^2+1, \quad 12=1\cdot 2^3+1\cdot 2^2,$

$$60=1\cdot 2^5+1\cdot 2^4+1\cdot 2^3+1\cdot 2^2$$

also

$$\nu=3, \quad E=0, \quad \varepsilon=0, \quad S(q)=2;$$

für $p=3$: $\quad 5=1\cdot 3^1+2, \quad 12=1\cdot 3^2+1\cdot 3^1$

$$60=2\cdot 3^3+2\cdot 3^1$$

also

$$\nu=1, \quad E=1, \quad \varepsilon=1, \quad S(q)=2;$$

für $p=5$: $\quad 5=1\cdot 5^1, \quad 12=2\cdot 5^1+2, \quad 60=2\cdot 5^2+2\cdot 5^1$

also

$$\nu=1, \quad E=0, \quad \varepsilon=0, \quad S(q)=4.$$

Der kleinste Wert des Ausdruckes $S(q)+\varepsilon$ ist demnach $\lambda=2$, also ist $(5!)^2$ die höchste im Quotienten $\frac{(60!)}{(12!)^5}$ aufgehende Potenz der Faktoriellen $5!$

14. E. Catalan hat in den *Nouv. Ann. de Math.* 2. sér. 13, 1874, p. 207 einen Satz bekannt gemacht, den er aus der Theorie der elliptischen Funktionen gewonnen, und hat ihn zugleich mit einem anderen auf p. 523 ebendaselbst nochmals gegeben. Wir erledigen zuerst diesen letzteren Satz, welcher aussagt, dafs, wenn m, n zwei relativ prime Zahlen sind, der Quotient

(57) $$Q=\frac{(m+n-1)!}{m!\,n!}$$

eine ganze Zahl sei. In der That kann man schreiben:

$$nQ = \frac{(m+1)(m+2)\cdots(m+n-1)}{1 \cdot 2 \cdot \cdots (n-1)}$$

$$mQ = \frac{(n+1)(n+2)\cdots(n+m-1)}{1 \cdot 2 \cdot \cdots (m-1)},$$

diese beiden Quotienten aber sind nach Nr. 12 ganze Zahlen. Wäre daher Q ein Bruch, der irreduktibel, auf seine einfachste Form gebracht, vorausgesetzt werden darf, so müfste jeder Primfaktor p seines Nenners sowohl gegen m wie gegen n sich heben, d. i. zugleich in diesen beiden Zahlen aufgehen, die doch nach Voraussetzung keinen gemeinsamen Teiler haben; mithin mufs Q eine ganze Zahl sein.

Der andere der **Catalan**schen Sätze besagt, dafs immer

$$\frac{(2m)!\,(2n)!}{m!\,n!\,(m+n)!} \tag{58}$$

ganzzahlig sei. Von diesem Satze hat der Verfasser (*Ztschr. f. Math. u. Phys.* 20, p. 161) einen Beweis gegeben, der in seine *Elem. der Zahlentheorie*, Lpzg. 1892, p. 37 Aufnahme gefunden hat. Bourguet hat denselben Satz unter einen allgemeineren subsumiert, den er jedoch nicht richtig ausgesprochen hat (*Nouv. Ann.* 2. sér. 14, 1875, p. 89; s. dazu Catalans Bemerkung ebendas. p. 179). Richtig gefafst lautet dieser, wie folgt: Der Quotient

$$\frac{(km_1)!\,(km_2)!\cdots(km_k)!}{m_1!\,m_2!\cdots m_k!\,(m_1+m_2+\cdots+m_k)!} \tag{59}$$

ist, wenn $k \geqq 2$ ist, eine ganze Zahl. Setzt man $k=2$, $m_1=m$, $m_2=n$, so ergiebt sich als Spezialfall der Satz von Catalan. Zum Beweise des allgemeinen bemerke man mit Bourguet, dafs irgend eine Primzahl p des Nenners nach der Legendreschen Formel (36) so oft im Zähler aufgeht, als die Summe

$$\sum_{i=1}^{\infty}\left[\frac{km_1}{p^i}\right] + \sum_{i=1}^{\infty}\left[\frac{km_2}{p^i}\right] + \cdots + \sum_{i=1}^{\infty}\left[\frac{km_k}{p^i}\right], \tag{60}$$

dagegen im Nenner so oft, als die Summe

$$\sum_{i=1}^{\infty}\left[\frac{m_1}{p^i}\right] + \sum_{i=1}^{\infty}\left[\frac{m_2}{p^i}\right] + \cdots + \sum_{i=1}^{\infty}\left[\frac{m_k}{p^i}\right] + \sum_{i=1}^{\infty}\left[\frac{m_1+m_2+\cdots+m_k}{p^i}\right] \tag{61}$$

beträgt. Es genügt zum Beweise des Satzes, zu zeigen, dafs die erstere Summe nicht kleiner ist, als die letztere, und dies wird offenbar der Fall sein, wenn es schon für das allgemeine Glied beider Summen zutrifft, wenn nämlich

$$\left[\frac{km_1}{p^i}\right] + \left[\frac{km_2}{p^i}\right] + \cdots + \left[\frac{km_k}{p^i}\right]$$
$$\geqq \left[\frac{m_1}{p^i}\right] + \left[\frac{m_2}{p^i}\right] + \cdots + \left[\frac{m_k}{p^i}\right] + \left[\frac{m_1+m_2+\cdots+m_k}{p^i}\right]$$

ist. Man setze nun $m_h = p^i q_h + r_h$, wo der Rest $r_h < p^i$; die Ungleichheit nimmt dann die Form an:

$$(k-2)(q_1 + q_2 + \cdots + q_k) + \left[\frac{k r_1}{p^i}\right] + \cdots + \left[\frac{k r_k}{p^i}\right]$$
$$\overline{\overline{>}} \left[\frac{r_1 + r_2 + \cdots + r_k}{p^i}\right]$$

und ist ersichtlich erfüllt, da schon dasjenige gröfste Ganze auf der linken Seite, in welchem r_h den gröfsten Wert hat, für sich allein der rechten Seite mindestens gleich ist.

15. Alle im Vorigen untersuchten Quotienten sind spezielle Fälle des folgenden:

$$\frac{u_1(x_i)!\, u_2(x_i)! \cdots u_m(x_i)!}{v_1(x_i)!\, v_2(x_i)! \cdots v_n(x_i)!}, \tag{62}$$

in welchem

$$u_h(x_i) = a_1^{(h)} x_1 + a_2^{(h)} x_2 + \cdots + a_r^{(h)} x_r$$
$$(\text{für } h = 1, 2, 3, \ldots m),$$
$$v_h(x_i) = b_1^{(h)} x_1 + b_2^{(h)} x_2 + \cdots + b_r^{(h)} x_r$$
$$(\text{für } h = 1, 2, 3, \cdots n)$$

$m + n$ in Bezug auf die positiven ganzen Zahlen $x_1, x_2, \ldots x_r$ lineare Funktionen mit nicht negativen ganzzahligen Koeffizienten sind. Diesen allgemeinen Quotienten hat E. Landau in einer kleinen Arbeit (*Nouv. Ann.* 3. sér., 19, 1900, sur les conditions de divisibilité d'un produit de factorielles par un autre) näher untersucht und als die notwendige und hinreichende Bedingung dafür, dafs er ganzzahlig sei, den Umstand ermittelt, dafs für alle Werte der y_i zwischen 0 und 1

$$\sum_{h=1}^{m} [u_h(y_i)] \overline{\overline{>}} \sum_{h=1}^{n} [v_h(y_i)]$$

sein müsse. Als ein neues Beispiel dieses Satzes, unter welchen, wie aus dem Vorigen leicht ersichtlich ist, die sämtlichen bisher betrachteten Fälle von Faktoriellen einbegriffen sind, giebt er den Quotienten an:

$$\frac{(4x_1)!\,(4x_2)!}{x_1!\, x_2!\, (2x_1 + x_2)!\, (x_1 + 2x_2)!}, \tag{63}$$

von dem wir durch seine Überlegungen zeigen wollen, dafs er für positive ganzzahlige Werte von x_1, x_2 eine ganze Zahl ist. Wir zeigen dazu zuvörderst, dafs für alle Werte y_1, y_2 zwischen 0 und 1 die Ungleichheit stattfindet:

$$[4y_1] + [4y_2] \overline{\overline{>}} [2y_1 + y_2] + [y_1 + 2y_2]. \tag{64}$$

Wegen der Symmetrie dieser Beziehung in Hinsicht der beiden Elemente y_1, y_2 dürfen wir bei solchem Nachweise voraussetzen, dafs $y_1 \leqq y_2$ sei. Da alsdann $2y_1 + y_2 \leqq y_1 + 2y_2$ ist, so wird, wenn man sich unter der gemachten Voraussetzung y_1, y_2 von 0 an wachsend denkt, zuerst $y_1 + 2y_2$ den ganzzahligen Wert 1 erreichen, dann wird bei weiterem Wachsen $2y_1 + y_2$ gleich 1 werden, dann $y_1 + 2y_2$ gleich 2, darauf wird $2y_1 + y_2$ diesen Wert erreichen, ferner aber weder $y_1 + 2y_2$ noch gar $2y_1 + y_2$ mehr gleich 3 werden können. Wir unterscheiden danach folgende Fälle:

1) sei $2y_1 + y_2 < 1$, $y_1 + 2y_2 < 1$; dann ist

$$[2y_1 + y_2] + [y_1 + 2y_2] = 0,$$

während $[4y_1] + [4y_2] \geqq 0$ sein mufs; die Ungleichheit (64) ist erfüllt;

2) sei $2y_1 + y_2 < 1$, $1 \leqq y_1 + 2y_2 < 2$; dann ist

$$[2y_1 + y_2] = 0, \quad [y_1 + 2y_2] = 1,$$

ferner aber, da schon $2y_1 + 4y_2 \geqq 2$ ist, a fortiori $[4y_1 + 4y_2] \geqq 2$; und, da $[a + b]$ entweder gleich $[a] + [b]$ oder um eine Einheit gröfser ist, findet sich

$$[4y_1] + [4y_2] \geqq 1,$$

also die Ungleichheit (64) erfüllt;

3) sei $2y_1 + y_2 \geqq 1$, $1 < y_1 + 2y_2 < 2$; dann ist

$$[2y_1 + y_2] = 1, \quad [y_1 + 2y_2] = 1,$$

ferner folgt sogleich $3y_1 + 3y_2 > 2$ also $[4y_1 + 4y_2] \geqq 2$; ist aber $[4y_1 + 4y_2] > 2$, so ist

$$[4y_1] + [4y_2] \geqq 2$$

also die Ungleichheit (64) erfüllt; ist dagegen $[4y_1 + 4y_2] = 2$, so wäre $4y_1 + 4y_2 < 3$, und da $4y_1 + 2y_2 \geqq 2$ ist, wäre $2y_2 < 1$, $4y_1 > 1$, also auch $4y_2 > 1$, demnach

$$[4y_1] + [4y_2] \geqq 2,$$

die Ungleichheit (64) also wieder erfüllt;

4) sei $2 > 2y_1 + y_2 > 1$, $2 \leqq y_1 + 2y_2 < 3$; dann ist

$$[2y_1 + y_2] = 1, \quad [y_1 + 2y_2] = 2,$$

ferner findet sich $3y_1 + 3y_2 > 3$, mithin $[4y_1 + 4y_2] \geqq 4$, $[4y_1] + [4y_2] \geqq 3$, die Ungleichheit (64) also erfüllt;

5) endlich sei $2y_1 + y_2 \geqq 2$, $2 < y_1 + 2y_2 < 3$; dann ist

$$[2y_1 + y_2] = 2, \quad [y_1 + 2y_2] = 2,$$

ferner $3y_1 + 3y_2 > 4$, $4y_1 + 4y_2 > \frac{16}{3} > 5$, also $[4y_1 + 4y_2] \geqq 5$,

$$[4y_1] + [4y_2] \geqq 4,$$

die Ungleichheit (64) ist also wieder erfüllt.

Nachdem dies bewiesen worden, betrachte man irgend welche positive ganze Zahlen P, x_1, x_2 und setze

$$x_1 = Pq_1 + r_1, \quad x_2 = Pq_2 + r_2,$$

wo q_1, q_2 positive ganze Zahlen, r_1, r_2 ebenfalls ganze Zahlen sind, welche positiv und kleiner als P. Hiernach findet man

$$\left[\frac{4x_1}{P}\right] + \left[\frac{4x_2}{P}\right] = 4q_1 + 4q_2 + \left[\frac{4r_1}{P}\right] + \left[\frac{4r_2}{P}\right]$$

$$\left[\frac{x_1}{P}\right] + \left[\frac{x_2}{P}\right] + \left[\frac{2x_1 + x_2}{P}\right] + \left[\frac{x_1 + 2x_2}{P}\right]$$

$$= 4q_1 + 4q_2 + \left[\frac{2r_1 + r_2}{P}\right] + \left[\frac{r_1 + 2r_2}{P}\right],$$

der Unterschied beider Ausdrücke aber ist, da $y_1 = \frac{r_1}{P}$, $y_2 = \frac{r_2}{P}$ zwischen 0 und 1 liegen, dem vorausgeschickten Satze zufolge, welche positive ganze Zahl auch unter P verstanden werde, nicht negativ. Hieraus schliefst man für jede Primzahl p, indem man $P = p^i$ wählt, die Ungleichheit:

$$\sum_{i=1}^{\infty}\left[\frac{4x_1}{p^i}\right] + \sum_{i=1}^{\infty}\left[\frac{4x_2}{p^i}\right]$$

$$\geqq \sum_{i=1}^{\infty}\left[\frac{x_1}{p^i}\right] + \sum_{i=1}^{\infty}\left[\frac{x_2}{p^i}\right] + \sum_{i=1}^{\infty}\left[\frac{2x_1 + x_2}{p^i}\right] + \sum_{i=1}^{\infty}\left[\frac{x_1 + 2x_2}{p^i}\right],$$

d. h. jede Primzahl p geht im Zähler des Quotienten (63) mindestens ebenso oft auf, wie im Nenner desselben, der Quotient ist also gleich einer ganzen Zahl. — Ein weiteres Beispiel des allgemeinen Satzes s. *Nouv. Ann.* (4) 1, juin 1901, p. 282.

16. Wir schliefsen hier noch einen Satz an, welchen Liouville (*Journ. de Math.*, 2. sér., 2, 1857, p. 277) bewiesen hat; Moreau, der ihn auf gleiche Weise herleitet (*Nouv. Ann.*, 2. sér., 11, 1872, p. 172) schreibt ihn Mathieu zu. Nach diesem Satze kann ein Produkt aufeinanderfolgender Zahlen:

$$m(m+1)(m+2)\cdots(m+n-1) \tag{65}$$

keine Quadratzahl sein, wenn in der Reihe der Faktoren eine Primzahl auftritt. Zum Beweise ist jedoch ein Hilfssatz erforderlich, der bisher nur durch Betrachtungen einer sehr viel höheren Art hat festgestellt werden können, nämlich der von Tschebischeff gegebene Satz: Wenn die ganze Zahl $a > 3$ ist, liegt zwischen den Grenzen a und $2a - 2$ mindestens eine Primzahl. Setzen wir ihn voraus, so mufs, wenn unter den Faktoren von (65) überhaupt eine Primzahl auftritt, für die gröfste von ihnen — sie heifse p — die Ungleichheit bestehen: $m + n - 1 < 2p$, denn

sonst gäbe es zwischen p und $m+n-1$ gewifs noch eine Primzahl und p wäre nicht die gröfste Primzahl unter den Faktoren von (65). Da demnach die Faktoren

$$m(m+1)\cdots(p-1), \quad (p+1)(p+2)\cdots(m+n-1)$$

dieses Produktes nicht durch p aufgehen, so ist das Produkt dann durch p, aber nicht durch p^2 teilbar, kann demnach keine Quadratzahl sein.

Setzt man $m>4$ und $n>m-5$ voraus, so ist das Produkt (65) stets von einer Quadratzahl verschieden; denn alsdann ist $m-1>3$ und zwischen $m-1$ und $2(m-1)-2=2m-4$ also auch zwischen $m-1$ und $m+n>2m-5$ d. i. in der Reihe der Faktoren des Produktes (65) liegt wenigstens eine Primzahl und die Bedingung des vorigen Satzes ist erfüllt.

Da in der Reihe $1, 2, 3, \ldots, n$ jedenfalls sich Primzahlen befinden, so schliefst man insbesondere: Die Faktorielle $n!$ ist niemals eine Quadratzahl.

Offenbar bestehen bezüglich des Produktes

$$(2m+1)(2m+3)\cdots(2m+2n-1)$$

ganz ähnliche Sätze. —

Drittes Kapitel.

Reste und Kongruenzen.

1. Im vorigen Kapitel haben wir mittels der fundamentalen Thatsache, dafs in Bezug auf eine gegebene ganze Zahl n jede andere ganze Zahl m in die Form

$$m = qn + r, \quad 0 \overline{\gtrless} r < n \tag{1}$$

gesetzt werden kann, den Nachweis geführt, dafs jeder Modulus der Zahlenreihe (Z) von der Form (nz) sei, und haben aus diesem Umstande die Sätze von der Teilbarkeit der ganzen Zahlen gewonnen. Jetzt kehren wir zu jener fundamentalen Formel wieder zurück, indem wir unser Hauptaugenmerk auf den Rest r in ihr richten wollen.

Bildet man die Formel für zwei Zahlen m', m'':

$$m' = q'n + r', \quad m'' = q''n + r'',$$

so können die Reste r', r'' einander gleich oder von einander verschieden sein; je nach diesen Fällen ist der Unterschied

$$m' - m'' = (q' - q'')n + (r' - r'') \tag{2}$$

eine Zahl des Moduls (nz), nämlich ein Vielfaches von n, oder nicht; denn, damit der Ausdruck (2) für $m' - m''$ durch n aufgehe, ist notwendig und hinreichend, dafs $r' - r''$ teilbar sei durch n, d. h., da dieser Unterschied numerisch kleiner ist als n, dafs $r' = r''$ sei.

Man nennt nun zwei Zahlen m', m'', deren Differenz eine Zahl des Modulus (nz) ist, einander nach diesem Modulus — kürzer (mod. n) — kongruent, in Zeichen:

$$m' \equiv m'' \pmod{n}. \tag{3}$$

Diese Definition sowie die entsprechende Bezeichnung rührt von Gaufs her (*Disquis. Arithm. art.* 1 u. 2), während die fragliche Beziehung selbst freilich schon vordem häufig genug in Betracht gezogen worden ist. Dem Vorigen zufolge sind zwei Zahlen m', m'' (mod. n) kongruent oder inkongruent, jenachdem sie in Bezug auf den Divisor n gleichrestig sind oder nicht. In Verallgemeinerung des Ausdruckes „Rest" nennt man deshalb auch wohl jede der kongruenten Zahlen m', m'' den Rest der anderen (mod. n).

Zwei Zahlen m', m'', welche (mod. n) ein- und derselben dritten Zahl m kongruent sind, sind es auch unter einander; denn, gehören die Differenzen $m' - m$, $m'' - m$ beide dem Modulus (nz) an, so thut's auch, der Definition eines Modulus gemäfs, der Unterschied

$$(m' - m) - (m'' - m) = m' - m''.$$

Hiernach lassen sich sämtliche ganze Zahlen in Klassen verteilen der Art, dafs die Zahlen derselben Klasse zu je zweien kongruent, dagegen zwei Zahlen verschiedener Klassen einander inkongruent sind (mod. n). Jede Klasse kongruenter Zahlen wird auch eine Restklasse genannt und kann durch eine beliebige der ihr angehörigen Zahlen repräsentiert werden. Da jede Zahl (mod. n) einen der Reste $0, 1, 2, 3, \cdots, n-1$ läfst, mithin einer dieser Zahlen kongruent sein mufs, ist die Anzahl der Restklassen nur endlich und zwar beträgt sie, da zwei jener Reste (mod. n) nicht kongruent sein können, ohne identisch zu sein, genau n. Wählt man aus jeder dieser Restklassen nach Belieben eine Zahl als ihren Repräsentanten aus, nimmt also irgend welche n unter einander inkongruente Zahlen, so heifst das System dieser Repräsentanten ein vollständiges Restsystem (mod. n). Solcher Restsysteme giebt es mithin unendlich viele. Z. B. dürfen dafür die Reste

$$0, 1, 2, 3, \ldots n-1$$

gewählt werden, welche, da sie die kleinsten positiven — genauer: nicht negativen — Zahlen der repräsentierten Restklassen sind, das System der kleinsten positiven Reste heifsen. Ist n ungerade, so sind die n Zahlen

$$-\frac{n-1}{2},\ -\frac{n-3}{2},\ \cdots -2,\ -1,\ 0,\ 1,\ 2,\ \cdots \frac{n-3}{2},\ \frac{n-1}{2}$$

zu je zweien inkongruent, sie bilden demnach auch ein vollständiges Restsystem, dasjenige der absolut kleinsten Reste; ähnlich könnte man für ein gerades n das System

$$-\frac{n}{2},\ -\frac{n-2}{2},\ \cdots -2,\ -1,\ 0,\ 1,\ 2,\ \cdots \frac{n-2}{2},\ \frac{n}{2}$$

wählen, in welchem jedoch die erste Zahl der letzten kongruent und demnach eine Klasse doppelt repräsentiert wäre, sodafs nach Belieben eine dieser beiden Zahlen gestrichen werden müfste; u. s. w.

Ist d ein Teiler von n und die Differenz $m'-m''$ eine Zahl des Modulus (nz) d. i. ein Vielfaches von n, so ist sie auch ein Vielfaches von d, also eine Zahl des Modulus (dz), mit andern Worten: aus $m' \equiv m''$ (mod. n) folgt auch $m' \equiv m''$ (mod. d). Gehört daher m' selbst zum Modulus (dz), so gehört auch die mit m' (mod. n) kongruente Zahl m'' demselben Modulus an; hat also eine Zahl einer Restklasse mit dem Modulus n den gemeinsamen Teiler d, so hat ihn jede andere Zahl dieser Restklasse ebenfalls. Was für jeden bestimmten mit n gemeinsamen Teiler gilt, das gilt auch für den gröfsten von ihnen. Ist insbesondere eine Zahl einer Restklasse relativ prim zum Modulus, so sind alle übrigen Zahlen derselben Restklasse es auch. Nimmt man daher aus einem vollständigen Restsysteme (mod. n) diejenigen Repräsentanten heraus, welche prim sind gegen n, so enthalten die zugehörigen Restklassen nur relative Primzahlen zu n und enthalten diese zugleich sämtlich, sie stellen daher die sämtlichen gegen n primen Zahlen in Restklassen verteilt dar. Die Repräsentanten dieser relativ primen Restklassen (mod. n), die wieder auf unendlich viel Arten gewählt werden können, bilden ein sogenanntes reduziertes Restsystem (mod. n); man erhält z. B. ein solches, wenn man aus den Resten $0, 1, 2, 3, \cdots n-1$ diejenigen herausnimmt, welche prim gegen n sind. Ist demnach $\varphi(n)$*) die Anzahl der Zahlen, welche $< n$ und prim gegen n sind, so besteht jedes reduzierte Restsystem (mod. n) aus je $\varphi(n)$ unter einander inkongruenten und gegen n primen Zahlen.

2. Die Zahlen, welche mehreren Moduln (nz), $(n'z)$, ... gemeinsam sind, bilden selbst einen Modulus, denn, sind ν', ν'' zwei

---

*) Das Funktionszeichen $\varphi(n)$ für die gedachte Anzahl rührt von Gaufs her, der es in seinen *Disqu. Ar. art.* 38 zuerst in die Mathematik einführte; doch bezeichnet man diese Funktion vielfach als Eulersche Funktion, da Euler als Erster ihren allgemeinen Wert für eine in Primzahlpotenzen zerlegte Zahl n angegeben hat (s. *Petrop. N. Comment.* 8, 1760/61, p. 74 = *Comm. Arithm. coll.* 1, p. 274).

solcher Zahlen, so gehören nach der Definition eines Modulus auch $\nu' \pm \nu''$ jedem dieser Moduln zugleich an. Ist daher N das kleinste der den gegebenen Moduln gemeinsamen Elemente, so ist ihre Gesamtheit der Modulus (Nz). Alle gemeinsamen Elemente sind aber die gemeinsamen Vielfachen von $n, n', \ldots$, und daher unter allen diesen N das kleinste. Aus dieser Betrachtung ergiebt sich der Satz: Ist $m' \equiv m''$ nach jeder der Zahlen $n, n', \ldots$ als Modulus, und ist N das kleinste gemeinsame Vielfache der letztern, so ist auch $m' \equiv m''$ (mod. N). Sind mithin die Zahlen $n, n', \ldots$ zu je zweien relativ prim, so folgt aus den Kongruenzen

$$m' \equiv m'' \text{ (mod. } n), \quad m' \equiv m'' \text{ (mod. } n'), \ldots$$

auch die Kongruenz

$$m' \equiv m'' \text{ (mod. } nn' \ldots).$$

Ferner erkennt man die Richtigkeit nachstehenden Satzes:

Aus

$$a \equiv b, \quad a' \equiv b' \text{ (mod. } n)$$

folgt

$$\left.\begin{aligned} a \pm a' &\equiv b \pm b' \\ aa' &\equiv bb' \end{aligned}\right\} \text{ (mod. } n).$$

In der That, gehören die Differenzen $a - b$, $a' - b'$ dem Modulus (nz) an, so auch deren Summe und deren Differenz $(a + a') - (b + b')$ resp. $(a - a') - (b - b')$; desgleichen die Vielfachen $(a - b)\,a'$ und $(a' - b')\,b$ der Elemente $a - b$, $a' - b'$ und folglich deren Summe $aa' - bb'$.

Hiernach lassen sich Kongruenzen, welche nach demselben Modulus stattfinden, durch Addition, Subtraktion und Multiplikation unter einander verbinden gerade wie Gleichungen; dagegen gilt für die Division nicht völlig das Gleiche. Hat man nämlich die Kongruenz

$$ma \equiv mb \text{ (mod. } n), \tag{4}$$

so folgt daraus nicht allezeit die Kongruenz

$$a \equiv b \text{ (mod. } n), \tag{5}$$

sondern, wenn d den gröfsten gemeinsamen Teiler von m, n bedeutet, nur diese:

$$a \equiv b \left(\text{mod. } \frac{n}{d}\right).$$

In der That ergiebt sich letztere aus der Teilbarkeit von $m(a - b)$ durch n oder von $\frac{m}{d}(a - b)$ durch $\frac{n}{d}$, da $\frac{m}{d}$, $\frac{n}{d}$ relative Primzahlen sind. Nur dann folgt also aus (4) die Kongruenz (5), wenn der Multiplikator m und der Modulus n teilerfremd sind.

Aus diesen einfachsten Kongruenzsätzen läfst sich sogleich der allgemeinere folgern: Ist $f(x)$ eine ganze und ganzzahlige Funktion von x:

$$f(x) = ax^{\alpha} + a_1 x^{\alpha-1} + \cdots + a_{\alpha-1}x + a_{\alpha},$$

wo die Koeffizienten a_i ganze Zahlen bedeuten, so ist

$$f(m') \equiv f(m'') \pmod{n},$$

so oft

$$m' \equiv m'' \pmod{n}$$

ist. In der That folgt dann auch $m'^h \equiv m''^h$ für jeden positiven ganzzahligen Exponenten h, daher auch $a_{\alpha-h} \cdot m'^h \equiv a_{\alpha-h} \cdot m''^h$ und daraus mittels des Additionssatzes die behauptete Kongruenz.

3. Der so erhaltene allgemeine Satz, der die vielfachste Verwendung findet, ist z. B. die eigentliche Quelle all' der mehr oder weniger bekannten oder nützlichen Regeln, nach denen man die Teilbarkeit einer dekadischen Zahl durch eine andere solche Zahl zu beurteilen vermag. Ist nämlich p irgend eine Zahl, die zur Grundzahl eines Ziffernsystems genommen werde, so kann jede ganze Zahl m, wie im vorigen Kapitel gezeigt ist, in die Form

$$(6) \quad m = ap^h + a_1 p^{h-1} + a_2 p^{h-2} + \cdots + a_{h-2} \cdot p^2 + a_{h-1} \cdot p + a_h$$

gesetzt werden, in welcher die Koeffizienten a_i nichtnegative ganze Zahlen $< p$ sind. Ist nun $p \equiv r \pmod{n}$, so ergiebt sich nach dem gedachten Satze

$$(7) \qquad m \equiv ar^h + a_1 r^{h-1} + \cdots + a_{h-2} r^2 + a_{h-1} r + a_h \pmod{n}$$

und demnach m teilbar oder nicht teilbar durch n, jenachdem es die rechte Seite der vorigen Kongruenz ist oder nicht ist. Insbesondere nimmt die Formel (7) für $p = n + 1$ resp. $p = n - 1$, welchen Annahmen der Wert $r = 1$ resp. $r = -1$ entspricht, die Gestalt:

$$m \equiv a + a_1 + \cdots + a_{h-1} + a_h \pmod{p-1}$$

resp.

$$m \equiv (-1)^h a + (-1)^{h-1} a_1 + \cdots - a_{h-1} + a_h \pmod{p+1}$$

an.

Hieraus fliefsen für die dekadischen Zahlen, bei denen $p = 10$ ist, die bekannten Regeln für die Teilbarkeit einer Zahl durch 9 und durch 11: eine Zahl ist teilbar durch 9 oder nicht, jenachdem ihre Quersumme d. i. die Summe ihrer Ziffern es ist oder nicht ist; und sie ist teilbar durch 11 oder nicht, jenachdem der Unterschied zwischen der Summe ihrer an gerader Stelle stehenden und der Summe ihrer an ungerader Stelle stehenden Ziffern es ist oder nicht ist.

In allgemeineren Fällen mufs man, statt die Ziffern einzeln zu nehmen, sie in Gruppen von je zwei, drei, u. s. w. Ziffern zusammen-

fassen. Ist nämlich $p^k \equiv 1 \pmod{n}$, so folgt offenbar aus (6) folgende Kongruenz:

$$\begin{aligned} m \equiv & (a_h + a_{h-1}p + \cdots + a_{h-k+1}p^{k-1}) \\ & + (a_{h-k} + a_{h-k-1}p + \cdots + a_{h-2k+1}p^{k-1}) \pmod{n}, \\ & + \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \end{aligned}$$

während, falls $p^k \equiv -1 \pmod{n}$ ist, sich

$$\begin{aligned} m \equiv & (a_h + a_{h-1}p + \cdots + a_{h-k+1}p^{k-1}) \\ & - (a_{h-k} + a_{h-k-1}p + \cdots + a_{h-2k+1}p^{k-1}) \quad \text{mod. } n) \\ & + \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \end{aligned}$$

ergiebt. So folgt z. B. für $p = 10$ d. i. für den Fall dekadischer Zahlen, da $10^2 \equiv 1 \pmod{11}$ ist, die Regel: Bildet man aus einer dekadischen Zahl andere, indem man von der letzten Ziffer an immer je zwei Ziffern zusammenfafst, so läfst, durch 11 geteilt, die gegebene Zahl den gleichen Rest, wie die Summe der abgeleiteten Zahlen und ist daher gleichzeitig mit dieser Summe teilbar oder nicht teilbar durch 11, z. B. die Zahl 7359132 gleichzeitig mit der Summe $7 + 35 + 91 + 32$.

Ferner ist $10^3 + 1 = 7 \cdot 11 \cdot 13$; bildet man also aus einer dekadischen Zahl andere, indem man von der letzten Ziffer an immer je drei Ziffern zu einer Zahl vereinigt, so läfst, durch 7, 11, 13 geteilt, die gegebene Zahl den gleichen Rest, wie der Unterschied zwischen der Summe der an ungerader Stelle stehenden und der Summe der an gerader Stelle stehenden abgeleiteten Zahlen, und ist demnach gleichzeitig mit diesem Unterschiede teilbar oder nicht teilbar durch jene Zahlen. Z. B. liefert so die Zahl

$$3594872156$$

die folgenden:

$$3, \ 594, \ 872, \ 156,$$

für welche der gedachte Unterschied -125 beträgt, eine Zahl, welche nach den Moduln 7, 11, 13 resp. die Reste 1, 7, 5 läfst, genau wie die gegebene Zahl.

Aus derselben Quelle entspringen die Resultate, welche O. Kefsler (*Ztschr. für Math. u. Phys.* 28, 1883, p. 60) betreffend die Teiler von Zahlen, welche durch Nebeneinanderstellung gleicher Zahlen entstehen, mitgeteilt hat.

Denkt man sich ferner die dekadische Zahl m durch Zusammenfassung ihrer Zehner, Hunderter u. s. w. in der Form dargestellt

$$m = 10a + a_0, \tag{8}$$

wählt irgend eine gegen die Zahl n prime ganze Zahl μ und setzt

$$10\mu \equiv \nu \pmod{n}, \tag{9}$$

indem man ν kleiner als n voraussetzt, so ergiebt sich

$$(10) \qquad \mu m \equiv \nu a + \mu a_0 \pmod{n},$$

also m gleichzeitig mit der anderen Zahl $m_1 = \nu a + \mu a_0$ teilbar oder nicht teilbar durch n. Z. B. ist $10 \cdot 9 \equiv -1$ nach jedem der Divisoren 7, 13; demnach ist m durch 7 teilbar oder nicht, jenachdem

$$-a + 9a_0 \quad \text{oder} \quad a - 2a_0$$

es ist oder nicht ist, und durch 13, jenachdem

$$-a + 9a_0 \quad \text{oder} \quad a + 4a_0$$

durch 13 teilbar ist oder nicht (vgl. Wertheim, *El. d. Zahlenth.* 1887, p. 32). Zu diesen Regeln s. Dietrichkeit, *Ztschr. f. Math. u. Phys.* 36, 1891, p. 64 und die Bemerkungen von R. H. van Dorsten und von K. Haas ebendas. 37, 1892, p. 58, 63. Eine andere vom Erstgenannten ebend. 36, p. 316 gegebene Regel beruht darauf, dafs in (6) die Potenzen von p durch ihre Reste ersetzt werden; s. dazu v. Dorsten ebend. 37, p. 192, wo auf R. Perrin, *C. R. de l'assoc. franç. pour l'advanc. des sciences* 1889, 2. partie, p. 24—38 verwiesen wird. Man mag bemerken, dafs, je komplizierter derartige Regeln ausfallen, um so eher darauf verzichtet und besser die unmittelbare Division versucht werden kann*).

4. Zurückkehrend zu dem Schlufssatze der Nr. 2 wird man zu der Frage geführt, welche Reste die dort betrachtete ganze, ganzzahlige Funktion $f(x) \pmod{n}$ lassen kann. Da man den fraglichen Rest mit dem konstanten Gliede der Funktion zusammenfassen kann, kommt diese Frage auf die andere zurück, ob eine gegebene ganze, ganzzahlige Funktion

$$(11) \qquad f(x) = ax^\alpha + a_1 x^{\alpha-1} + \cdots + a_{\alpha-1}x + a_\alpha \equiv 0 \pmod{n}$$

sein kann oder nicht, ob es nämlich ganze Zahlen x giebt, welche dieser Kongruenz genügen? Solche Zahlen, wenn sie vorhanden sind, heifsen Lösungen der Kongruenz; da aber, wenn $x = m$ eine solche ist, zugleich auch die unendlich vielen Zahlen $m' \equiv m \pmod{n}$ Lösungen sein werden, in Kongruenzen aber Zahlen, welche nach deren Modulus kongruent sind, nur die Rolle einer einzigen Zahl spielen, so nennt man alle, derselben Zahl m kongruenten Lösungen einer Kongruenz eine Wurzel derselben, in Zeichen:

$$\text{die Wurzel } x \equiv m \pmod{n}.$$

Hier besteht für den Fall, dafs der Modulus n eine Primzahl p ist, ein wichtiger Satz, zu dessen Aufstellung noch nötig ist, den Grad

*) Vgl. zu diesen Angaben die neuestens erschienene kleine Abhandlung von G. Loria: *carattere di divisibilità per un numero intero qualunque*, *Rendiconti della R. Accad. dei Lincei* 10, 1901, p. 150.

einer Kongruenz zu definieren. Offenbar darf man in (11), ohne die etwaigen Lösungen der Kongruenz zu beeinflussen, Glieder fortlassen oder hinzufügen, deren Koeffizienten durch den Modulus $n = p$ teilbar sind; der Exponent nun des höchsten Gliedes, dessen Koeffizient durch p nicht teilbar ist, heifse der Grad der Kongruenz. Der gemeinte Satz besagt dann Folgendes:

Eine Kongruenz, deren Modulus eine Primzahl ist, kann nie mehr Wurzeln haben, als ihr Grad beträgt.

Wir leiten diesen Satz, welchen zuerst L. Euler (*Petrop. Comm. nov.* 18, 1733, p. 93 = *Comm. Arithm.* 1, p. 519) für die spezielle Kongruenz $x^n \equiv 1 \pmod{p}$, später Lagrange (*Berl. Ac. Hist.* 24, 1770 — année 1768 — p. 192) allgemein bewiesen hat, folgendermafsen her:

Offenbar ist der Satz richtig für Kongruenzen des ersten Grades, denn, hätte eine solche:

$$ax + a_1 \equiv 0 \pmod{p},$$

zwei Wurzeln $x \equiv m'$, $x \equiv m''$, so folgte aus

$$am' + a_1 \equiv 0, \quad am'' + a_1 \equiv 0$$

auch $a(m' - m'') \equiv 0 \pmod{p}$ d. h. $a(m' - m'')$ und, da a prim ist gegen p, auch $m' - m''$ teilbar durch p, also $m' \equiv m'' \pmod{p}$ gegen die Voraussetzung. Nehmen wir daher ferner an, der Satz gelte für Kongruenzen, deren Grad $< \alpha$ ist, und zeigen ihn dann auch für solche vom Grade α, so ist er damit allgemein bewiesen. Gesetzt aber, die Kongruenz

$$ax^\alpha + a_1 x^{\alpha-1} + \cdots + a_{\alpha-1} x + a_\alpha \equiv 0 \pmod{p} \tag{12}$$

vom Grade α hätte mehr als α Wurzeln, also mindestens $\alpha + 1$, welche $m, m_1, m_2, \ldots m_\alpha$ seien, so genügten die Wurzeln $m_1, m_2, \ldots m_\alpha$ nicht nur der vorstehenden, sondern ersichtlich auch der folgenden Kongruenz:

$$a(x - m_1)(x - m_2) \cdots (x - m_\alpha) \equiv 0 \pmod{p},$$

demnach auch der anderen, durch beider Verbindung entstehenden:

$$ax^\alpha + a_1 x^{\alpha-1} + \cdots + a_\alpha - a(x - m_1) \cdots (x - m_\alpha) \equiv 0 \pmod{p},$$

deren Grad höchstens noch $\alpha - 1$ sein kann. Der Voraussetzung nach kann die letztere nur identisch sein d. h. die Koeffizienten der nach Potenzen von x geordneten Funktion müssen teilbar durch p, oder, was dasselbe sagt, die Koeffizienten gleich hoher Potenzen zur Rechten und Linken in der nachstehenden Kongruenz

$$ax^\alpha + a_1 x^{\alpha-1} + \cdots + a_\alpha \equiv a(x - m_1) \cdots (x - m_\alpha) \pmod{p}$$

müssen (mod. p) kongruent sein. Demnach hat die Kongruenz (12) genau dieselben Wurzeln wie diese andere:

$$a(x - m_1)(x - m_2) \cdots (x - m_\alpha) \equiv 0 \pmod{p}.$$

Während aber nach der Annahme die erstere durch $x \equiv m$ erfüllt wird, leistet m der letzteren kein Genüge, da das Produkt

$$a(m - m_1)(m - m_2) \cdots (m - m_\alpha),$$

dessen erster Faktor prim ist zu p, nur dann durch p teilbar sein könnte, wenn es einer der übrigen Faktoren d. h., wenn m einer der Zahlen $m_1, m_2, \ldots m_\alpha$ kongruent wäre (mod. p), was der Annahme zuwider. Hiermit ist gezeigt, dafs die Kongruenz (12) vom Grade α nicht mehr als α Wurzeln besitzen kann, wie behauptet war.

5. Ist vorher gezeigt, dafs die Kongruenz ersten Grades

$$ax + a_1 \equiv 0 \text{ (mod. } p)$$

oder, wie wir sie jetzt lieber schreiben wollen, indem wir $-a_1 = c$ setzen,

$$ax \equiv c \text{ (mod. } p), \tag{13}$$

nicht mehr als eine Wurzel besitzen kann, so soll nun nachgewiesen werden, dafs sie diese eine immer auch besitzt. Hierzu betrachten wir die allgemeinere Kongruenz

$$ax \equiv c \text{ (mod. } n) \tag{14}$$

unter der Voraussetzung, dafs a prim sei gegen n, und zeigen, dafs eine solche stets eine Wurzel hat.

Sei, dies zu zeigen,

$$r_1, r_2, r_3, \ldots r_n \tag{15}$$

irgend ein vollständiges Restsystem (mod. n). Multipliziert man seine Glieder mit einer zu n primen Zahl a, so stellen die Produkte

$$ar_1, ar_2, ar_3, \ldots ar_n \tag{16}$$

wieder ein solches dar; denn von diesen n Zahlen können keine zwei, etwa ar_1, ar_2 (mod. n) kongruent d. i. $a(r_1 - r_2)$ teilbar durch n sein, da r_1, r_2 inkongruent, also $r_1 - r_2$ nicht durch n teilbar sein kann. Eine einzige der Zahlen (16), etwa ar_h, mufs demnach derselben Restklasse angehören wie c, und folglich

$$ar_h \equiv c \text{ (mod. } n),$$

d. i. $x \equiv r_h$ eine und zugleich die einzige Wurzel von (14) sein.

Da in dem vollständigen Restsysteme (16) offenbar diejenigen und nur diejenigen Zahlen ar_h prim gegen n sind, welche den zu n primen Zahlen r_h der Reihe (15), d. i. den Repräsentanten eines reduzierten Restsystemes (mod. n) entsprechen, so ergiebt sich sogleich der weitere Satz:

Multipliziert man die Glieder eines beliebigen reduzierten Restsystems (mod. n) mit einer zum Modulus primen

Zahl, so stellen die erhaltenen Produkte wieder ein reduziertes Restsystem (mod. n) dar.

Nehmen wir nun an, in der Kongruenz (14) habe a mit dem Modulus n einen von 1 verschiedenen gröfsten gemeinsamen Teiler d. Da dieser Teiler, welch' ganzzahliger Wert auch für x gewählt werde, immer in ax aufgeht, so mufs, wenn die Kongruenz (14) bestehen soll, dieser gemeinsame Teiler von n und ax auch der mit ax kongruenten Zahl c gemeinsam sein. Die Möglichkeit der Kongruenz (14) erfordert also, dafs c durch den gröfsten gemeinsamen Teiler d von a und n aufgehe.

Angenommen, diese Bedingung sei erfüllt, sodafs man setzen darf

$$a = da', \quad n = dn', \quad c = dc',$$

wo nun a', n' relativ prime Zahlen sein werden, so besagt die Kongruenz (14), dafs

$$ax - c = d(a'x - c') \quad \text{durch} \quad n = dn',$$

d. h. dafs $a'x - c'$ durch n' teilbar oder dafs

$$a'x \equiv c' \pmod{n'}$$

sei; sie hat daher genau dieselben Lösungen, wie diese letztere Kongruenz. Da diese nun dem Vorigen zufolge eine Wurzel besitzt, so sei dieselbe $x \equiv \xi \pmod{n'}$, d. h. $x = \xi + n'z$, unter z jede ganze Zahl verstanden. Der angegebene Wert von x erfüllt dann auch die Kongruenz (14) oder ist für jeden der Werte von z eine Lösung derselben. Indessen sind diese unendlich vielen Lösungen hier nicht eine einzige Wurzel von (14), nämlich nicht sämtlich kongruent (mod. n). Setzt man nämlich $z = dq + r$, wo r jede der Zahlen $0, 1, 2, \cdots d-1$ bedeuten darf, so wird

$$x = \xi + n'r + nq,$$

d. i.

$$x \equiv \xi + \frac{n}{d} \cdot r \pmod{n} \tag{17}$$

$$(\text{für} \quad r = 0, 1, 2, \cdots d-1)$$

und diese d verschiedenen Werte sind inkongruent, denn, damit für zwei verschiedene der angegebenen Werte von r, etwa r', r''

$$\xi + \frac{n}{d} r' \equiv \xi + \frac{n}{d} r'' \pmod{n}$$

würde, müfste $\frac{n}{d}(r' - r'')$ durch n, d. h. $r' - r''$ durch d teilbar sein, was nicht sein kann. Somit zerfallen die unendlich vielen Lösungen der Kongruenz (14), die wir nachgewiesen haben, in die d Wurzeln (17). Man findet demnach: Ist die als notwendig erkannte Bedingung für die Möglichkeit der Kongruenz (14) erfüllt, so besitzt dieselbe d Wurzeln.

Da diese Kongruenz erfordert, dafs $c - ax$ ein Vielfaches von n, gleich ny sei, und umgekehrt erfüllt ist, wenn dies der Fall, so ist sie, wenn man der Symmetrie wegen den Modulus n lieber mit b bezeichnet, mit der unbestimmten (**Diophantischen**) Gleichung ersten Grades:

$$ax + by = c \tag{18}$$

vollständig gleichbedeutend. Zur Auflösbarkeit der letzteren ist mithin notwendig und hinreichend, dafs der gröfste gemeinsame Teiler d von a, b auch in c aufgehe; in dieser Voraussetzung hat man für x die Werte

$$x = \xi + \frac{b}{d} z$$

zu setzen, wo ξ irgend ein Wert ist, für welchen $c - a\xi$ ein Vielfaches von b, etwa gleich $b\eta$, mithin

$$a\xi + b\eta = c \tag{19}$$

ist; und man findet, jenen Werten von x entsprechend,

$$by = c - ax = c - a\xi - \frac{ab}{d} z = b\eta - b \cdot \frac{a}{d} z,$$

also

$$y = \eta - \frac{a}{d} z.$$

Die allgemeine Auflösung der Gleichung (18) ist also

$$x = \xi + \frac{b}{d} z, \quad y = \eta - \frac{a}{d} z,$$

wo ξ, η **eine** Auflösung derselben und z jeden ganzzahligen Wert bedeutet. Hiermit bestätigt sich nochmals die Möglichkeit der unbestimmten Gleichung

$$ax + by = d$$

und insbesondere, wenn a, b relativ prim sind, diejenige der Gleichung

$$ax + by = 1,$$

die wir in Nr. 2 des vorigen Kapitels aus den fundamentalsten Betrachtungen bereits erkannt haben.

Die Möglichkeit der letzteren Gleichung oder der Kongruenz

$$ax \equiv 1 \pmod{b}$$

im Falle teilerfremder Zahlen a, b läfst ersehen, dafs in diesem Falle eine Zahl a' vorhanden ist so beschaffen, dafs

$$aa' \equiv 1 \pmod{b}.$$

Diese Zahl a' heifst nach Euler (Gaufs, *D. A.* art. 77) eine zu a (mod. b) associierte Zahl; offenbar ist umgekehrt a eine zu

a' (mod. b) associirte Zahl und zusammen heifsen sie socii (mod. b). Auch setzt man

(20) $$a' \equiv \frac{1}{a}, \quad a \equiv \frac{1}{a'} \pmod{b}.$$

6. Wir geben nun einige Anwendungen der gewonnenen Resultate. Als erste derselben werde die Zerlegung eines irreduktiblen Bruches in sogenannte **Partialbrüche** hergeleitet. Denkt man den Nenner des Bruches $\frac{m}{n}$ in zwei teilerfremde Faktoren: $n = ab$, zerfällt, so ist dem Letztgesagten zufolge die unbestimmte Gleichung

(21) $$ax + by = m$$

stets auflösbar, denn, ist x_0, y_0 eine Auflösung der Gleichung

$$ax_0 + by_0 = 1,$$

so hat man nur zu setzen: $x = mx_0$, $y = my_0$. Aus (21) aber folgt

$$\frac{x}{b} + \frac{y}{a} = \frac{m}{n}$$

und, wenn man die kleinsten nichtnegativen Reste von y, x resp. (mod. a), (mod. b) mit α, β bezeichnet, die fernere Gleichung

(22) $$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + h,$$

wo h eine positive oder negative ganze Zahl bedeutet, die Zähler α, β aber kleiner als a, b resp. und positiv sind; in der That kann keine dieser Zahlen Null sein, da, wenn z. B. $\alpha = 0$ wäre, sich

$$m = (\beta + hb)\, a$$

ergäbe d. h. $\frac{m}{n}$ gegen die Voraussetzung kein irreduktibler Bruch wäre. Auch sind α, β zu den Nennern a, b resp. prim; denn hätten z. B. β, b den von 1 verschiedenen gröfsten gemeinsamen Teiler δ, sodafs $\beta = \beta'\delta$, $b = b'\delta$ gesetzt werden kann, so ergäbe sich

$$m = (\alpha b' + \beta' a + hab')\,\delta, \quad n = ab'\delta$$

und $\frac{m}{n}$ wäre wieder kein irreduktibler Bruch.

Ersetzt man b in (22) durch ein Produkt zweier relativ primer Zahlen: bc, d. h. setzt man n als das Produkt von drei, zu je zweien relativ primen Faktoren, $n = abc$, voraus, so läfst sich $\frac{\beta}{b}$ ähnlich zerlegen wie $\frac{m}{n}$ und man findet

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + h,$$

wo h wieder eine ganze Zahl, die Brüche aber irreduktible Brüche bedeuten mit Zählern, welche positiv und kleiner als die Nenner sind. So fortfahrend gelangt man zu folgendem Satze:

Ist $\frac{m}{n}$ ein irreduktibler Bruch und $n = abc \ldots$ eine Zerlegung seines Nenners in mehrere zu je zweien relativ prime Faktoren, so läfst sich der Bruch $\frac{m}{n}$ stets in Partialbrüche mit den Nennern $a, b, c, \ldots$ nach folgender Formel zerlegen:

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \cdots + h; \tag{23}$$

hierin bezeichnen $\alpha, \beta, \gamma \ldots$ positive mit bezug auf den entsprechenden Nenner prime und kleinere Zahlen, als er, und h eine ganze Zahl.

Solche Zerlegung ist aber auch nur auf eine einzige Art möglich. Wäre nämlich auch

$$\frac{m}{n} = \frac{\alpha'}{a} + \frac{\beta'}{b} + \frac{\gamma'}{c} + \cdots + h',$$

so erhielte man durch Gleichsetzung dieses Ausdrucks mit dem Ausdrucke (23) und Multiplikation mit $\frac{n}{a}$ die Beziehung:

$$\frac{\alpha' - \alpha}{a} \cdot bc \cdots \text{ gleich einer ganzen Zahl},$$

folglich $\alpha' - \alpha$ teilbar durch a, und, da α, α' beide kleiner sind als a, $\alpha' = \alpha$; unterdrückt man beiderseits die gleichen Brüche $\frac{\alpha}{a}$, $\frac{\alpha'}{a}$, und behandelt die übrige Gleichung auf ähnliche Weise, indem man sie mit $\frac{n}{ab}$ multipliziert, so findet sich $\beta' = \beta$, ähnlich dann $\gamma' = \gamma$ u. s. w., endlich also auch $h' = h$ und somit die völlige Übereinstimmung beider Partialbruchzerlegungen.

Besonders beachtenswert wird diese Zerlegung, wenn man den Nenner n in seine Primzahlpotenzfaktoren zerlegt denkt. Seien diese dann

$$a = p^i, \quad b = q^k, \quad c = r^l, \cdots, \tag{24}$$

so kann man den Zahlen $\alpha, \beta, \gamma, \ldots$ die nachstehenden Gestalten geben:

$$\begin{aligned} \alpha &= \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots + \alpha_{i-1} p^{i-1} \\ \beta &= \beta_0 + \beta_1 q + \beta_2 q^2 + \cdots + \beta_{k-1} q^{k-1} \\ \gamma &= \gamma_0 + \gamma_1 r + \gamma_2 r^2 + \cdots + \gamma_{l-1} r^{l-1} \\ &\cdots\cdots\cdots\cdots\cdots \end{aligned} \tag{25}$$

in denen die Koeffizienten nichtnegative Zahlen kleiner als $p, q, r, \ldots$ resp. bedeuten. Demnach nimmt die Zerlegung (23) folgendes Aussehen an:

$$
\begin{aligned}
\frac{m}{n} &= \frac{m}{p^i q^k r^l \ldots} \\
&= \frac{\alpha_0}{p^i} + \frac{\alpha_1}{p^{i-1}} + \cdots + \frac{\alpha_{i-1}}{p} \\
&+ \frac{\beta_0}{q^k} + \frac{\beta_1}{q^{k-1}} + \cdots + \frac{\beta_{k-1}}{q} \qquad (26) \\
&+ \frac{\gamma_0}{r^l} + \frac{\gamma_1}{r^{l-1}} + \cdots + \frac{\gamma_{l-1}}{r} \\
&+ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot + h.
\end{aligned}
$$

Man nennt sie die Zerlegung des irreduktiblen Bruches $\frac{m}{n}$ in **einfache** Brüche.

Auch eine solche ist nur auf eine Weise möglich. Denn zunächst folgt aus dem Bestehen einer Gleichung von der Form (26), daſs

$$\frac{p^i q^k r^l \ldots m}{n}$$

eine ganze Zahl, daſs also, da m, n relativ prim vorausgesetzt wurden, n in $p^i q^k r^l \ldots$ enthalten ist und daher aus keinen anderen Primfaktoren zusammengesetzt sein kann als aus $p, q, r, \ldots$ und letztere Primfaktoren auch nicht öfter enthalten kann, als resp. $i, k, l, \ldots$-mal. Enthielte aber n z. B. den Primfaktor p nur $g < i$-mal, so würde schon $\frac{p^g q^k r^l \ldots m}{n}$ und daher nach der vorausgesetzten Gleichung von der Form (26) auch

$$\frac{\alpha_0 + \alpha_1 p + \cdots + \alpha_{i-g-1} \cdot p^{i-g-1}}{p^{i-g}}$$

eine ganze Zahl sein müssen, was nicht sein kann, da der Zähler kleiner ist als der Nenner. Ist somit festgestellt, daſs bei jeder Darstellung des Bruchs $\frac{m}{n}$ in der Gestalt (26) $p^i q^k r^l \cdots = n$ sein muſs, so stimmt jede solche Darstellung mit der eindeutig bestimmten Zerlegung (23), bei welcher $a, b, c, \ldots$ die Werte (24) haben und $\alpha, \beta, \gamma, \ldots$ in die Form (25) gesetzt sind, überein, und da auch diese letzteren Formeln nur eindeutig aufgestellt werden können, ist die Darstellung (26) ebenfalls nur auf eine einzige Weise möglich.

7. Eine zweite Anwendung machen wir auf die Auflösung der Aufgabe, eine Zahl x zu finden, welche nach gegebenen Moduln gegebene Reste läſst, also einer Reihe von Kongruenzen:

$$x \equiv \alpha \ (\text{mod.}\ a), \quad x \equiv \beta \ (\text{mod.}\ b), \quad x \equiv \gamma \ (\text{mod.}\ c), \cdots \qquad (27)$$

genügt. Um eine solche Zahl, wenn möglich, zu finden, kann man successive x so bestimmen, daſs sie der ersten, sodann auch der zweiten, ferner auch der dritten Kongruenz Genüge leistet, u. s. w. Nun sind zunächst

$$x = \alpha + ay,$$

wo y jede ganze Zahl bedeutet, alle Zahlen, welche die erste der Kongruenzen (27) erfüllen. Man hat demnach jetzt y so zu wählen, dafs auch die zweite erfüllt, d. i. dafs

$$(28) \qquad ay \equiv \beta - \alpha \pmod{b}$$

wird. Dies ist nach Nr. 5 stets möglich, wenn a, b relativ prim; im entgegengesetzten Falle, wenn also a, b einen von 1 verschiedenen gröfsten gemeinsamen Teiler d haben, ist aber die vorige Kongruenz und somit die gestellte Aufgabe nicht immer möglich, erfordert vielmehr, dafs $\beta - \alpha$ gleichfalls teilbar sei durch d. Gesetzt, letztere Bedingung sei erfüllt, so ist die Kongruenz (28) mit der anderen:

$$\frac{a}{d} y \equiv \frac{\beta - \alpha}{d} \left(\text{mod. } \frac{b}{d}\right)$$

gleichbedeutend, welche auflösbar ist und eine Wurzel $y \equiv \eta \left(\text{mod. } \frac{b}{d}\right)$ besitzt; setzt man dementsprechend $y = \eta + \frac{b}{d} z$ also

$$x = \alpha + a\eta + \frac{ab}{d} z,$$

so giebt dieser Ausdruck für alle ganzzahligen z die sämtlichen gleichzeitigen Lösungen der beiden ersten Kongruenzen (27). Um daher auch noch der dritten von ihnen zu genügen, hat man z so zu wählen, dafs

$$\alpha + a\eta + \frac{ab}{d} z \equiv \gamma \pmod{c}$$

oder

$$\frac{ab}{d} z \equiv \gamma - \alpha - a\eta \pmod{c}$$

werde. Diese Wahl ist möglich, sobald $\frac{ab}{d}$ prim gegen c ist, was gewifs der Fall, wenn a, b prim gegen c sind; entgegengesetztenfalls tritt als neue Bedingung, unter welcher die vorige Kongruenz also auch die gestellte Aufgabe allein möglich ist, das Erfordernis auf, dafs $\gamma - \alpha - a\eta$ durch den gröfsten gemeinsamen Teiler δ von $\frac{ab}{d}$ und c gleichfalls teilbar sei. Ist diese Bedingung wieder erfüllt, so ist die vorhergehende Kongruenz identisch mit der anderen:

$$\frac{ab}{d\delta} z \equiv \frac{\gamma - \alpha - a\eta}{\delta} \left(\text{mod. } \frac{c}{\delta}\right),$$

welche lösbar ist und eine Wurzel $z \equiv \zeta \left(\text{mod. } \frac{c}{\delta}\right)$ besitzt; alle Zahlen x folglich, welche den ersten drei der Kongruenzen (27) genügen, werden dann gegeben durch die Formel

$$x = \alpha + a\eta + \frac{ab}{d} \zeta + \frac{abc}{d\delta} u,$$

wo u eine ganze Zahl ist, u. s. w. fort.

Man entnimmt dieser Analyse, dafs die Kongruenzen (27) immer gleichzeitig auflösbar sind, wenn ihre Moduln zu je zweien relativ prim sind.

Allgemein aber gelangt man, so oft sie lösbar sind, zu einer Beziehung

$$x \equiv \xi,$$

welche nach der Zahl $\frac{abc\ldots}{d\delta\ldots}$ d. h. nach dem kleinsten gemeinsamen Vielfachen der gegebenen Moduln als Modulus stattfindet und sämtliche Lösungen der gestellten Aufgabe zusammenfafst; der Modulus ist das Produkt der gegebenen Moduln in dem Falle, wo sie zu je zweien teilerfremd sind.

Die Aufgabe läfst sich vereinfachen, indem man die Moduln $a, b, c, \ldots$ in ihre Primzahlpotenzen auflöst. Ist nämlich $a = p^i p'^{i'} \ldots$, so darf zunächst die erste der Kongruenzen (27) durch das System der folgenden:

$$(29) \qquad x \equiv \alpha \ (\text{mod.}\, p^i), \quad x \equiv \alpha \ (\text{mod.}\, p'^{i'}), \ldots$$

ersetzt werden; denn, ist $x - \alpha$ teilbar durch a, so ist's auch teilbar durch die einzelnen Potenzen p^i, $p'^{i'}, \ldots$, und umgekehrt. Ähnlich ersetze man die übrigen Kongruenzen (27) durch solche, deren Moduln die resp. $b, c, \ldots$ zusammensetzenden Primzahlpotenzen sind. Ist nun eine Primzahl vorhanden, etwa p, die in zwei oder mehreren der Moduln $a, b, c, \ldots$ aufgeht, etwa in a, b, so kommen zwei oder mehr Kongruenzen von der Form

$$(30) \qquad x \equiv \alpha \ (\text{mod.}\, p^i), \quad x \equiv \beta \ (\text{mod.}\, p^k), \ldots$$

vor. Hier ist von den Exponenten i, k der eine gleich oder gröfser als der andere, etwa $i \geqq k$, folglich mufs dann umsomehr

$$x \equiv \alpha \ (\text{mod.}\, p^k)$$

sein, und diese Bedingung, mit der zweiten der voraufgehenden verglichen, liefert als notwendiges Erfordernis für die Möglichkeit der Aufgabe die Bedingung

$$\beta \equiv \alpha \ (\text{mod.}\, p^k).$$

Ist sie aber erfüllt, so darf die zweite der Kongruenzen (30) als in der ersten schon mitenthalten fortgelassen werden. Verfährt man so bezüglich aller als Moduln auftretenden Primzahlpotenzen, so bleibt, falls sich die Aufgabe nicht als unlösbar herausstellt, von den Kongruenzen (29) und den analogen anderen, in die wir die Kongruenzen (27) aufgelöst haben, nur eine Reihe von Kongruenzen von der Form:

$$x \equiv \alpha \ (\text{mod.}\, p^i), \ldots, \quad x \equiv \beta \ (\text{mod.}\, q^k), \ldots, \quad x \equiv \gamma \ (\text{mod.}\, r^l), \ldots$$

übrig, deren Moduln Potenzen verschiedener Primzahlen also relativ prim sind, welche daher stets eine Lösung gestatten.

Soll z. B. gleichzeitig

$$x \equiv 9 \pmod{1400}, \quad x \equiv 37 \pmod{252}, \quad x \equiv 64 \pmod{135}$$

sein, so darf man diese Forderungen, da

$$1400 = 2^3 \cdot 5^2 \cdot 7, \quad 252 = 2^2 \cdot 3^2 \cdot 7, \quad 135 = 5 \cdot 3^3$$

ist, durch das System der nachstehenden ersetzen:

$$\begin{array}{lll} x \equiv \;\, 9 \pmod{2^3}, & x \equiv \;\, 9 \pmod{5^2}, & x \equiv \;\, 9 \pmod{7} \\ x \equiv 37 \pmod{2^2}, & x \equiv 37 \pmod{3^2}, & x \equiv 37 \pmod{7} \\ x \equiv 64 \pmod{5}, & x \equiv 64 \pmod{3^3}. & \end{array}$$

Durch ihre Vergleichung miteinander entspringen die Möglichkeitsbedingungen

$$\begin{aligned} 37 &\equiv \;\, 9 \pmod{7} \\ 64 &\equiv 37 \pmod{3^2} \\ 64 &\equiv \;\, 9 \pmod{5} \\ 37 &\equiv \;\, 9 \pmod{2^2}, \end{aligned}$$

welche sämtlich erfüllt sind, und das vorige System von Kongruenzen reduziert sich auf das einfachere:

$$x \equiv 9 \pmod{2^3}, \quad x \equiv 9 \pmod{5^2}, \quad x \equiv 9 \pmod{7}, \quad x \equiv 64 \pmod{3^3}$$

oder noch einfacher auf das folgende:

$$x \equiv 9 \pmod{1400}, \quad x \equiv 64 \pmod{27}.$$

Der ersteren Kongruenz genügen die Zahlen $x = 9 + 1400y$, und nun ist y so zu wählen, dafs

$$1400y \equiv 55 \pmod{27}$$

oder dafs $23y \equiv 1 \pmod{27}$ werde, was geschieht, wenn $y \equiv 20 \pmod{27}$ gesetzt wird. Hiernach ergiebt sich die Lösung der gestellten Aufgabe in der Kongruenz

$$x \equiv 28\,009 \pmod{37\,800};$$

der Modulus $37\,800 = 2^3 \cdot 5^2 \cdot 7 \cdot 3^3$ ist das kleinste gemeinsame Vielfache der drei gegebenen Moduln, und man überzeugt sich sofort, dafs die Zahl 28009 den gestellten Kongruenzen genügt.

8. Falls die Moduln der Kongruenzen (27) zu je zweien relativ prime Zahlen sind, kann man eine Methode zu ihrer Lösung*) angeben, welche vor der successive fortschreitenden mancherlei Vorzüge besitzt, wenn sie auch anscheinend ein Umweg ist. Zu ihren Vor-

*) Diese Lösung findet sich angegeben in Gaufs *Disqu. Ar.* art. 36; es ist aber höchst beachtenswert, dafs sie schon vor vielen Jahrhunderten den Chinesen bekannt gewesen, nämlich bereits von dem chinesischen Mathematiker Sun Tsze in seinem Werke *Ta yen* entwickelt worden ist; vgl. darüber die interessanten Abhandlungen von K. L. Biernatzki und von L. Matthiessen im *Journ. f. Math.* 52, 1886, p. 59 und 91, 1881, p. 254.

zügen gehört, dafs sie in Bezug auf die gestellten Kongruenzen symmetrisch verfährt. Der bezeichnete Umweg aber besteht in der vorläufigen Bestimmung gewisser Hilfszahlen. Man suche nämlich Zahlen $r, s, t, \ldots$, welche bezw. die Bedingungen erfüllen:

$$r \equiv 1 \pmod{a}, \quad \equiv 0 \pmod{b}, \quad \equiv 0 \pmod{c}, \ldots$$
$$s \equiv 0 \pmod{a}, \quad \equiv 1 \pmod{b}, \quad \equiv 0 \pmod{c}, \ldots$$
$$t \equiv 0 \pmod{a}, \quad \equiv 0 \pmod{b}, \quad \equiv 1 \pmod{c}, \ldots$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

Jedes dieser Systeme ist dem Obigen zufolge auflösbar und man findet z. B. r, indem man $r = r'bc\ldots$ setzt und r' der Kongruenz

$$r'bc\ldots \equiv 1 \pmod{a}$$

gemäfs wählt. Hat man diese Hilfszahlen ermittelt, so ergiebt sich die Lösung der gegebenen Kongruenzen unmittelbar durch die folgende Beziehung:

$$x \equiv \alpha r + \beta s + \gamma t + \cdots \pmod{abc\ldots}. \tag{31}$$

In der That, wenn x ihr gemäfs gewählt ist, so ist auch

$$x \equiv \alpha r + \beta s + \gamma t + \cdots \pmod{a}$$

d. i. nach dem Verhalten der Hilfszahlen gegen den Modulus a

$$x \equiv \alpha \pmod{a};$$

gleicherweise kommt $x \equiv \beta \pmod{b}$, $x \equiv \gamma \pmod{c}, \ldots$; umgekehrt wird eine Zahl, welche $\alpha \pmod{a}$ kongruent ist, es auch mit

$$\alpha r + \beta s + \gamma t + \cdots$$

$\pmod{a}$ sein, und folglich wird eine Zahl x, welche die gestellten Kongruenzen erfüllt, mit diesem Ausdrucke nach jedem der Moduln $a, b, c, \ldots$ und, weil diese zu je zweien teilerfremd sind, auch $\pmod{abc\ldots}$ kongruent sein, w. z. b. w.

Hätte man beispielsweise die Kongruenzen

$$x \equiv 3 \pmod{17}, \quad x \equiv 1 \pmod{12}, \quad x \equiv 4 \pmod{5}$$

zu lösen, so bestimme man die Hilfszahlen r, s, t durch die Bedingungen:

$$r \equiv 1 \pmod{17}, \quad \equiv 0 \pmod{12}, \quad \equiv 0 \pmod{5}$$
$$s \equiv 0 \pmod{17}, \quad \equiv 1 \pmod{12}, \quad \equiv 0 \pmod{5}$$
$$t \equiv 0 \pmod{17}, \quad \equiv 0 \pmod{12}, \quad \equiv 1 \pmod{5}.$$

Man setze also $r = 60r'$ und wähle r' so, dafs $60r' \equiv 1$ oder einfacher $9r' \equiv 1 \pmod{17}$ wird; dies geschieht durch $r' = 2$, also ist $r = 120$. Ferner setze man $s = 85s'$ und wähle s' so, dafs $85s' \equiv 1$ oder einfacher $s' \equiv 1 \pmod{12}$ werde; dies geschieht für $s' = 1$ und man findet $s = 85$. Endlich setze man $t = 204t'$ uud bestimme t' so, dafs $204t' \equiv 1$ oder $4t' \equiv 1 \pmod{5}$ werde, was für $t' = 4$ er-

füllt wird und $t = 816$ ergiebt. Nunmehr erhält man sogleich die Auflösungen der gegebenen Kongruenzen durch die Formel

$$x \equiv 3 \cdot 120 + 1 \cdot 85 + 4 \cdot 816 \pmod{1020}$$

d. i. $x \equiv 3709 \equiv 649 \pmod{1020}$.

Der wesentlichste Vorzug dieser neuen Methode vor der früher angegebenen besteht darin, dafs sie sämtliche Aufgaben der gedachten Art, bei denen die Moduln $a, b, c, \ldots$ dieselben bleiben, die geforderten Reste $\alpha, \beta, \gamma, \ldots$ aber beliebig variieren, durch die allgemeine Formel (31) auf einmal erledigt, indem man eben in diese Formel nur für $\alpha, \beta, \gamma, \ldots$ die verlangten Reste zu setzen hat. Auf solche Weise gelangt man aber auch zu allgemeinen Sätzen, die auszusprechen nützlich ist. Läfst man nämlich $\alpha, \beta, \gamma, \ldots$ in der Formel (31) **vollständige** Restsysteme nach ihren bezüglichen Moduln $a, b, c, \ldots$ durchlaufen, so erhält man $abc\ldots$ Werte des Ausdruckes

$$\alpha r + \beta s + \gamma t + \cdots,$$

welche ebenfalls ein **vollständiges** Restsystem (mod. $abc\ldots$) repräsentieren. In der That sind alle diese Werte (mod. $abc\ldots$) inkongruent; denn, wäre für zwei Systeme $\alpha', \beta', \gamma', \ldots$ und $\alpha'', \beta'', \gamma'', \ldots$, deren entsprechende Zahlen α', α''; β', β''; γ', γ''; ... nicht durchweg (mod. a), (mod. b), (mod. c), ... resp. kongruent sind,

$$\alpha' r + \beta' s + \gamma' t + \cdots \equiv \alpha'' r + \beta'' s + \gamma'' t + \cdots \pmod{abc\ldots},$$

so fände diese Kongruenz auch nach jedem der Moduln $a, b, c, \ldots$ statt, und wegen des Verhaltens der Hilfszahlen zu diesen Moduln erhielte man dann

$$\alpha' \equiv \alpha'' \pmod{a}, \quad \beta' \equiv \beta'' \pmod{b}, \quad \gamma' \equiv \gamma'' \pmod{c}, \ldots$$

gegen die Voraussetzung.

Man kann sich diese Theorie zu Nutze machen, um die Auflösung einer Kongruenz ersten Grades zu erleichtern. Sei eine solche:

$$mx \equiv n \pmod{M},$$

bei welcher m, M als relative Primzahlen vorausgesetzt werden, zu lösen, und $M = abc\ldots$ irgend eine Zerlegung des Modulus M in Faktoren, welche zu je zweien relativ prim sind. Dann ist zunächst die gegebene Kongruenz mit dem folgenden Systeme gleichbedeutend

$$mx \equiv n \pmod{a}, \quad mx \equiv n \pmod{b}, \quad mx \equiv n \pmod{c}, \ldots;$$

denn jede Zahl x, welche der gegebenen Kongruenz genügt, erfüllt notwendig auch diese abgeleiteten, und da, wenn $mx - n$ teilbar ist einzeln durch $a, b, c, \ldots$, es auch teilbar ist durch $M = abc\ldots$, auch umgekehrt. Sind nun

$$x \equiv \alpha \pmod{a}, \quad x \equiv \beta \pmod{b}, \quad x \equiv \gamma \pmod{c}, \ldots$$

die Wurzeln der einzelnen abgeleiteten Kongruenzen, so leistet die Zahl

$$x \equiv \alpha r + \beta s + \gamma t + \cdots \pmod{M}$$

allen abgeleiteten Kongruenzen Genüge, ist mithin die Wurzel der gegebenen Kongruenz.

Werden hier $a, b, c, \ldots$ als die verschiedenen Primzahlpotenzen gewählt, aus denen sich M zusammensetzt, so führt diese Betrachtung die Auflösung der gegebenen Kongruenz auf mehrere ähnliche Kongruenzen von der Form

$$mx \equiv n \pmod{p^k}$$

zurück. Ist nun schon die Kongruenz

$$mx \equiv n \pmod{p^{k-1}}$$

gelöst und $x \equiv \xi \pmod{p^{k-1}}$ ihre Wurzel d. h. sind $x = \xi + p^{k-1}z$ für alle ganzzahligen z alle ihre Lösungen, so läfst sich z so wählen, dafs

$$m \cdot p^{k-1}z \equiv n - m\xi \pmod{p^k}$$

also x eine Wurzel der Kongruenz (mod. p^k) wird; da nämlich $n - m\xi$ eine durch p^{k-1} teilbare ganze Zahl ist, hat man z nur durch die Kongruenz ersten Grades

$$mz \equiv \frac{n - m\xi}{p^{k-1}} \pmod{p}$$

zu bestimmen. Hiernach kommt offenbar die Kongruenz (mod. p^k) und somit allgemeiner jede gegebene Kongruenz ersten Grades auf solche zurück, deren Moduln Primzahlen sind.

9. Noch wichtiger ist für uns die Bemerkung, dafs der Ausdruck

$$\alpha r + \beta s + \gamma t + \cdots$$

ein **reduziertes** Restsystem (mod. $abc\ldots$) durchläuft, wenn $\alpha, \beta, \gamma, \ldots$ **reduzierte** Restsysteme in Bezug auf ihre Moduln $a, b, c, \ldots$ resp. durchlaufen.

Dafs die so erhaltenen $\varphi(a) \cdot \varphi(b) \cdot \varphi(c) \ldots$ Werte jenes Ausdruckes (mod. $abc\ldots$) inkongruent sind, folgt aus dem eben Bewiesenen; es erübrigt nur der Nachweis, dafs jeder dieser Werte prim ist gegen $abc\ldots$, sowie dafs auch umgekehrt jeder zu $abc\ldots$ prime Rest sich unter den bezeichneten Werten befindet. Hätte nun aber erstens einer dieser Werte

$$\alpha r + \beta s + \gamma t + \cdots$$

einen Primfaktor p gemeinsam mit $abc\ldots$, so sei dieser etwa ein solcher von a; dann müfste, da

$$\alpha r + \beta s + \gamma t + \cdots \equiv \alpha \pmod{a}$$

ist, auch α diesen Teiler mit a gemeinsam haben gegen die Voraussetzung. Zweitens ist nach dem in voriger Nr. gegebenen Satze

ein jeder, also auch jeder zu $abc\ldots$ prime Rest (mod. $abc\ldots$) einem Werte des Ausdrucks

$$\alpha r + \beta s + \gamma t + \cdots$$

kongruent, aber einem solchen, bei dem $\alpha, \beta, \gamma, \ldots$ prim sind resp. gegen $a, b, c, \ldots$; denn, hätte z. B. α einen Primteiler p mit a gemeinsam, so würde, da

$$\alpha r + \beta s + \gamma t + \cdots \equiv \alpha \pmod{a}$$

ist, auch der gedachte, diesem Ausdrucke (mod. $abc\ldots$) also auch (mod. a) kongruente Rest den Primteiler p mit a und also mit dem Modulus $abc\ldots$ gemeinsam haben d. h. nicht relativ prim gegen ihn sein.

Beachtet man nun, dafs die Anzahl der Glieder eines reduzierten Restsystems (mod. $abc\ldots$) durch die Funktion $\varphi(abc\ldots)$ bezeichnet wird, so ergiebt sich aus dem eben bewiesenen Satze sogleich folgende wichtige Beziehung:

$$\varphi(abc\ldots) = \varphi(a) \cdot \varphi(b) \cdot \varphi(c) \cdots, \tag{32}$$

so oft $a, b, c, \ldots$ zu je zweien relativ prim sind, insbesondere für zwei relativ prime Zahlen m, n die Beziehung

$$\varphi(mn) = \varphi(m) \cdot \varphi(n). \tag{32a}$$

Sie darf als die fundamentale Eigenschaft der Eulerschen φ-Funktion bezeichnet werden, weil man aus ihr für eine in ihre Primfaktoren zerlegte Zahl

$$n = p^a p_1^{a_1} p_2^{a_2} \ldots \tag{33}$$

ohne weiteres den entwickelten Ausdruck der Funktion $\varphi(n)$ gewinnt. Zunächst ist nämlich

$$\varphi(n) = \varphi(p^a) \cdot \varphi(p_1^{a_1}) \cdot \varphi(p_2^{a_2}) \cdots. \tag{34}$$

Nun sind aber in der Reihe der Zahlen $1, 2, 3, \ldots p^a$ diejenigen prim zum Modulus p^a, die keine Vielfachen von p sind; um sie und ihre Anzahl zu finden, mufs man also aus dieser Reihe die Vielfachen von p d. h. die Zahlen

$$1 \cdot p,\ 2 \cdot p,\ 3 \cdot p, \cdots p^{a-1} \cdot p$$

ausscheiden, deren Anzahl p^{a-1} beträgt, und man findet daher

$$\varphi(p^a) = p^a - p^{a-1} = p^{a-1} \cdot (p-1). \tag{34a}$$

Insbesondere ist für eine Primzahl p

$$\varphi(p) = p - 1. \tag{34b}$$

Hiernach ergiebt die Formel (34) sofort den allgemeinen Ausdruck

$$\varphi(n) = p^{a-1}(p-1) \cdot p_1^{a_1-1}(p_1 - 1) \cdot p_2^{a_2-1}(p_2 - 1) \cdots, \tag{35}$$

dem man auch die folgende Gestalt:

$$(35^{a})\qquad \varphi(n) = n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p_1}\right)\cdots = \frac{n}{p\,p_1\cdots}(p-1)(p_1-1)\cdots$$

geben kann (s. eine direkte Herleitung dieser Formel in Lejeune Dirichlets *Vorlesungen über Zahlentheorie*, herausg. von Dedekind).

Bei der Wichtigkeit der fundamentalen Beziehung (32^{a}) leiten wir dieselbe durch nachstehende Betrachtung noch einmal her. Man denke sich die Zahlen von 1 bis mn in folgender Weise in n Reihen angeordnet:

$$(36)\qquad \begin{array}{llll} 1, & 2, & 3, \cdots & m \\ m+1, & m+2, & m+3, \cdots & 2m \\ 2m+1, & 2m+2, & 2m+3, \cdots & 3m \\ \cdots & \cdots & \cdots & \cdots \\ (n-1)m+1, & (n-1)m+2, & \cdots\cdots & nm. \end{array}$$

Da die Glieder jeder dieser Reihen den entsprechenden der ersten (mod. m) kongruent sind, so werden diejenigen Kolonnen, welche den $\varphi(m)$ zu m primen Zahlen der ersten Reihe entsprechen, zusammen die zu m primen Zahlen des ganzen Systems (36) sein. Es kommt darauf an, diejenigen Zahlen dieser Kolonnen herauszugreifen, welche auch prim gegen n und demnach prim gegen mn sind. Nun bilden aber die Zahlen jeder Kolonne:

$$h,\ m+h,\ 2m+h,\ \cdots\ (n-1)m+h,$$

da m prim gegen n ist, ein vollständiges Restsystem (mod. n), in welchem $\varphi(n)$ Glieder gegen n prim sind. Da somit in jeder der gedachten $\varphi(m)$ Kolonnen je $\varphi(n)$ der gesuchten Zahlen vorhanden sind, giebt es deren im ganzen $\varphi(m)\cdot\varphi(n)$ und demnach ist ihre Anzahl

$$\varphi(mn) = \varphi(m)\cdot\varphi(n).$$

Man kann fragen, wie diese Formel zu verändern sei, um für nicht relativ prime Zahlen m, n giltig zu sein. Man bezeichne zu diesem Zwecke dann mit P das Produkt der verschiedenen Primfaktoren, welche m, n gemeinsam sind, mit M, N die Produkte der verschiedenen, nur in m resp. nur in n aufgehenden Primfaktoren. Dann ist nach (35^{a}) und (34^{b}) und (32^{a})

$$\varphi(m) = \frac{m}{PM}\cdot\varphi(P)\,\varphi(M)$$

$$\varphi(n) = \frac{n}{PN}\cdot\varphi(P)\,\varphi(N)$$

$$\varphi(mn) = \frac{mn}{PMN}\cdot\varphi(P)\,\varphi(M)\,\varphi(N)$$

also

$$(37)\qquad \varphi(mn) = \varphi(m)\,\varphi(n)\cdot\frac{P}{\varphi(P)}\cdot$$

Diese Formel läſst sich leicht auf ein Produkt von mehreren Faktoren ausdehnen. Sei $n = rs$ und P' das Produkt der verschiedenen Primfaktoren, welche r, s gemeinsam sind, so wird nach der gefundenen Formel

$$\varphi(n) = \varphi(r)\,\varphi(s) \cdot \frac{P'}{\varphi(P')}$$

also zunächst

$$\varphi(mrs) = \varphi(m)\,\varphi(r)\,\varphi(s) \cdot \frac{P}{\varphi(P)} \cdot \frac{P'}{\varphi(P')}$$

sein. Aber die Primfaktoren von P zerfallen in diejenigen, die nur m, r, in diejenigen anderen, die nur m, s und endlich in diejenigen wieder anderen, die allen drei Zahlen m, r, s, gemeinsam sind, und die Produkte aus den Primzahlen dieser einzelnen Kategorien sind zu je zweien relativ prim. Desgleichen zerfallen die Primfaktoren von P' in diejenigen, welche nur r und s, und in diejenigen, welche allen drei Zahlen m, r, s gemeinsam sind, und das Produkt aus den ersteren ist gegen das der letzteren prim. Bezeichnet man daher mit P_1 das Produkt aller verschiedenen Primzahlen, die nur je zweien der drei Zahlen m, r, s gemeinsam sind, mit P_2 das Produkt derjenigen, die in ihnen allen dreien aufgehen, so folgt nach der Grundeigenschaft der φ-Funktion nachstehende Verallgemeinerung der Formel (37):

$$(37^a) \qquad \varphi(mrs) = \varphi(m)\,\varphi(r)\,\varphi(s) \cdot \frac{P_1}{\varphi(P_1)} \cdot \left(\frac{P_2}{\varphi(P_2)}\right)^2,$$

und in ähnlicher Weise kann man zu noch gröſserer Allgemeinheit fortschreiten (s. Lucas *th. des nombres* p. 399).

10. Ist d irgend ein Teiler von n, also

$$(38) \qquad d = p^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \ldots,$$

wo

$$0 \leqq \alpha \leqq a, \quad 0 \leqq \alpha_1 \leqq a_1, \quad 0 \leqq \alpha_2 \leqq a_2, \ldots$$

zu denken ist, so findet sich nach Formel (35)

$$(39) \qquad \varphi(d) = p^{\alpha-1}(p-1) \cdot p_1^{\alpha_1-1}(p_1-1) \cdot p_2^{\alpha_2-1}(p_2-1) \cdots,$$

wobei man, so oft einer der Exponenten $\alpha, \alpha_1, \alpha_2 \ldots$ gleich 0 ist, den auf die entsprechende Primzahl bezüglichen Faktor der rechten Seite durch 1 zu ersetzen hat; daher kommt, wenn man die Summe dieser Ausdrücke bildet für jene sämtlichen Teiler, 1 und n inklusive,

$$\begin{aligned}\sum_d \varphi(d) = {} & [1 + (p-1) + p(p-1) + \cdots p^{a-1}(p-1)] \\ & \cdot [1 + (p_1-1) + p_1(p_1-1) + \cdots p_1^{a_1-1}(p_1-1)] \\ & \cdot [1 + (p_2-1) + p_2(p_2-1) + \cdots p_2^{a_2-1}(p_2-1)] \\ & \cdots\cdots\cdots\cdots\cdots\cdots\end{aligned}$$

d. i.

$$\sum_d \varphi(d) = p^{a} \cdot p_1^{a_1} \cdot p_2^{a_2} \cdots$$

oder

$$(40) \qquad \sum_d \varphi(d) = n.$$

Da gleichzeitig mit d auch der Quotient $\frac{n}{d}$ die Reihe sämtlicher Teiler von n, nur in umgekehrter Reihenfolge, durchläuft, darf diese Formel auch durch die andere:

$$(40^a) \qquad \sum_d \varphi\left(\frac{n}{d}\right) = n$$

ersetzt werden, und in dieser Gestalt läſst sie sich ohne Mühe aus der Bedeutung der Funktion $\varphi(n)$ selbst herleiten. In der That, fragen wir nicht sowohl nach der Anzahl der Zahlen in der Reihe

$$(41) \qquad 1, 2, 3, \ldots n,$$

welche prim gegen n sind d. i. den gröſsten gemeinsamen Teiler 1, sondern allgemeiner nach der Anzahl derjenigen, die den gröſsten gemeinsamen Teiler d mit n haben, so befinden sich diese Zahlen jedenfalls unter den durch d teilbaren Zahlen der Reihe (41) d. h. unter den Zahlen

$$1d,\ 2d,\ 3d, \cdots \frac{n}{d}d,$$

und irgend eine dieser Zahlen, hd, wird mit $n = \frac{n}{d}d$ dann und nur dann d zum gröſsten gemeinsamen Teiler haben, wenn h und $\frac{n}{d}$ relativ prim sind; ihre Anzahl ist also ebenso groſs, wie die Anzahl der Zahlen

$$1,\ 2,\ 3, \cdots \frac{n}{d},$$

welche prim gegen $\frac{n}{d}$ sind, also gleich $\varphi\left(\frac{n}{d}\right)$. Nun hat aber notwendig jede der Zahlen (41) eine und nur eine Zahl d von der Form (38) zum gröſsten gemeinsamen Teiler mit n; sie lassen sich demnach, indem man diejenigen von ihnen vereinigt, welche denselben gröſsten gemeinsamen Teiler d mit n haben, in Gruppen verteilen, deren jede resp. $\varphi\left(\frac{n}{d}\right)$ Glieder enthält; und somit muſs die Gesamtzahl n der Zahlen (41) der Summe all' dieser, den sämtlichen Teilern d von n entsprechenden Werte $\varphi\left(\frac{n}{d}\right)$ gleich sein, wie es Formel (40^a) aussagt.

Eine andere Formel, welche mit der letzteren eine gewisse Ähnlichkeit hat, nämlich die Formel

$$(42) \qquad n = \varphi(n) + \sum p^{a-1} \cdot \varphi\left(\frac{n}{p^a}\right) + \sum p^{a-1} p_1^{a_1-1} \varphi\left(\frac{n}{p^a p_1^{a_1}}\right) + \cdots,$$

in welcher die erste Summation sich auf alle verschiedenen Prim-

faktoren von n, die zweite auf alle ihre Kombinationen zu je zweien, u. s. w., erstreckt, gab Pepin und Moret-Blanc hat sie bestätigt (*Nouv. Ann.* 2. série, 14, 1875, p. 275, 371), indem er darauf aufmerksam machte, dafs die Gesamtheit aller Zahlen von 1 bis n in folgende Kategorien zerfällt:

1) in diejenigen, welche zu n prim sind und deren Anzahl $\varphi(n)$ ist;

2) in diejenigen, welche nur einen Primfaktor mit n gemeinsam haben und deren Anzahl durch die erste Summe in (42) bezeichnet wird, da z. B. diejenigen Zahlen, welche nur den Primfaktor p mit n gemeinsam haben, die Zahlen der Reihe

$$\begin{array}{lll} 1p, & 2p, & \cdots p^{a-1}\cdot p \\ (p^{a-1}+1)p, & (p^{a-1}+2)p, & \cdots 2p^{a-1}\cdot p \\ \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot \\ \left[p^{a-1}\left(\frac{n}{p^a}-1\right)+1\right]p, & & \cdots n \end{array}$$

sind, welche prim sind gegen $\frac{n}{p^a}$, deren es aber in jeder der p^{a-1} Kolonnen, deren Zahlen eine Reihe von der Form

$$h+0\cdot p^a,\; h+1\cdot p^a,\; h+2\cdot p^a, \cdots h+\left(\frac{n}{p^a}-1\right)p^a$$

bilden, jedesmal $\varphi\left(\frac{n}{p^a}\right)$ giebt;

3) in diejenigen, welche nur zwei Primfaktoren mit n gemeinsam haben, und deren Anzahl, wie man auf ähnliche Weise erkennt, durch die zweite der Summen in (42) ausgedrückt wird;

u. s. w. —

11. Die Funktion $\varphi(n)$ ist mehrfach verallgemeinert worden. Z. B. hat V. Schemmel (*Journ. f. Math.* 70, 1869, p. 191) darauf hingewiesen, dafs unter den Zahlen, welche kleiner als n und prim gegen n sind, sich eine Anzahl Gruppen von je $m < n$ aufeinanderfolgenden Zahlen befinden wird, z. B., wenn n eine Primzahl p ist, die $p - m$ Gruppen

$$\begin{array}{c} 1,\ 2,\ 3, \cdots m \\ 2,\ 3,\ 4, \cdots m+1 \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ p-m,\ p-m+1, \cdots p-1. \end{array}$$

Er hat diese Anzahl, die offenbar für $m = 1$ mit der Funktion $\varphi(n)$ identisch ist, mit $\varphi_m(n)$ bezeichnet und ihre fundamentalsten Eigenschaften, welche denjenigen der Eulerschen Funktion ganz analog sind, angegeben. L. Goldschmidt hat dann die Schemmelschen Sätze ausführlich bewiesen (*Ztschr. f. Math. u. Phys.* 39, 1894, p. 203). Diese Funktion $\varphi_m(n)$ ist jedoch selbst nur ein besonderer Fall einer noch allgemeineren, die von Lucas (*th. d. nombres,*

p. 402) betrachtet worden ist. Seien nämlich $e_1, e_2, \ldots e_k$ beliebige ganze Zahlen, so soll $\psi(n)$ die Anzahl der Zahlen h der Reihe $1, 2, 3, \ldots n$ bedeuten, für welche die Summen

$$(43) \qquad h + e_1,\ h + e_2, \cdots h + e_k$$

prim sind gegen n. Bei der Annahme $e_1 = 1,\ e_2 = 2, \cdots e_k = k < n$ sind die vorstehenden Summen k aufeinanderfolgende Zahlen, denen daher in der Reihe der Zahlen $1, 2, 3, \ldots n$ eine Gruppe von ebenfalls successiven, den ersteren (mod. n) kongruenten, also zu n primen Zahlen entspricht; und umgekehrt entspricht jeder Gruppe der letzteren Art ein Wert von h, für welchen die Zahlen (43) bei den angenommenen Werten der e_i prim sind gegen n; in dieser besonderen Annahme wird also die Funktion $\psi(n)$ zur Schemmelschen Funktion $\varphi_k(n)$. Nun kann man vor allem für die Funktion $\psi(n)$ dieselbe Grundeigenschaft nachweisen, welche für die Funktion $\varphi(n)$ in der Formel (32^a) ausgedrückt ist. Sind nämlich m, n zwei relativ prime Zahlen, so ist, wie behauptet wird,

$$(44) \qquad \psi(mn) = \psi(m) \cdot \psi(n).$$

Man kann dies bestätigen auf ganz demselben Wege, wie es zuletzt für die Gleichung (32^a) gethan worden ist; jedoch knüpfen wir lieber an die Theorie der Kongruenzen ersten Grades an. Wenn r, s zwei Hilfszahlen bezeichnen, welche den Kongruenzen

$$r \equiv 1 \pmod{m}, \quad r \equiv 0 \pmod{n}$$
$$s \equiv 0 \pmod{m}, \quad s \equiv 1 \pmod{n}$$

genügen, so durchläuft z nach der Formel

$$z \equiv rx + sy \pmod{mn}$$

ein vollständiges Restsystem (mod. mn), sobald darin x den Zahlen $1, 2, \ldots m$, und y den Zahlen $1, 2, \ldots n$ gleich gesetzt werden. Demnach kann man auch für jedes i

$$e_i \equiv r\xi_i + s\eta_i \pmod{mn}$$

setzen, woraus sich $e_i \equiv \xi_i \pmod{m}$, $e_i \equiv \eta_i \pmod{n}$ ergiebt, und man findet so

$$z + e_i \equiv r(x + \xi_i) + s(y + \eta_i) \pmod{mn}.$$

Nun wird $z + e_i$ relativ prim zu mn dann und nur dann, wenn zugleich $x + \xi_i$ oder, was dasselbe sagt, $x + e_i$ prim gegen m, und $y + \eta_i$ oder, was auf dasselbe hinauskommt, $y + e_i$ prim gegen n ist. Dies geschieht aber gleichzeitig mit Bezug auf alle $i = 1, 2, 3, \ldots k$ für $\psi(m)$ Werte x der Reihe $1, 2, 3, \ldots m$ und für $\psi(n)$ Werte y der Reihe $1, 2, 3 \ldots n$, und giebt also $\psi(m) \cdot \psi(n)$ als Anzahl der zulässigen Werte von z, welche andererseits durch $\psi(mn)$ zu bezeichnen ist, und so ergiebt sich die behauptete Formel (44).

Aus dieser Formel fliefst nun der Ausdruck der Funktion $\psi(n)$ für jede in Primzahlpotenzen zerlegte Zahl n. Sei zunächst n eine Primzahlpotenz: $n = p^a$. Dann sind unter den Zahlen der Reihe $1, 2, 3, \ldots n$, nämlich unter den Zahlen:

$$\begin{array}{l} 1, \quad 2, \quad 3, \cdots p-1, p \\ p+1, p+2, p+3, \cdots 2p-1, 2p \\ \cdots\cdots\cdots\cdots \\ (p^{a-1}-1)p+1, (p^{a-1}-1)p+2, \cdots p^a-1, p^a \end{array}$$

immer die in einer Kolonne befindlichen einander (mod. p) kongruent. Bezeichnet daher λ die Anzahl der (mod. p.) inkongruenten unter den Zahlen $e_1, e_2, \ldots e_k$ und $r_1, r_2 \ldots r_\lambda$ die Reste, die sie (mod. p) lassen, so werden ersichtlich die sämtlichen Summen (43) dann und nur dann prim gegen p also auch gegen $n = p^a$, wenn man h einem der $p - \lambda$ mit $-r_1, -r_2, \cdots -r_\lambda$ inkongruenten Reste (mod. p) oder irgend einer Zahl in der ihm entsprechenden Kolonne gleichsetzt. Somit findet sich sogleich

(45) $$\psi(p^a) = p^{a-1}(p-\lambda),$$

insbesondere also

(45ª) $$\psi(p) = p - \lambda.$$

Allgemein entspricht daher der Zahl $n = p^a p_1^{a_1} p_2^{a_2} \ldots$ der Wert

(46) $$\psi(n) = p^{a-1}(p-\lambda) \cdot p_1^{a_1-1}(p_1-\lambda_1) \cdot p_2^{a_2-1}(p_2-\lambda_2) \cdots,$$

wo die Zeichen $\lambda_1, \lambda_2, \ldots$ mit Bezug auf die Primzahlen $p_1, p_2, \ldots$ dieselbe Bedeutung haben, wie das Zeichen λ mit Bezug auf die Primzahl p.

Wählt man sämtliche Zahlen e_i gleich 0, so geht die Formel (46), wie es sein mufs, in den Ausdruck für die Eulersche Funktion über. Wird dagegen $e_1 = 1$, $e_2 = 2, \cdots e_k = k$ gesetzt und k kleiner angenommen als die sämtlichen Primfaktoren von n, so werden die Zahlen $\lambda, \lambda_1, \lambda_2, \ldots$ offenbar gleich k und man findet für die Schemmelsche Funktion $\varphi_k(n)$ den Ausdruck

(47) $$\varphi_k(n) = p^{a-1}(p-k) \cdot p_1^{a_1-1}(p_1-k) \cdots$$

Ist im Gegenteil k gleich oder gröfser als einer jener Primfaktoren, z. B. als p, so wird $\varphi_k(n) = 0$, denn dann enthalten die Zahlen (43) bei der Annahme $e_1 = 1$, $e_2 = 2, \cdots e_k = k$ in sich ein vollständiges Restsystem (mod. p) und können für keinen Wert von h sämtlich prim gegen p also auch nicht gegen n sein.

Bildet man die Funktion $\psi(n)$ für jedes Argument n, das ein Teiler

$$d = p^a p_1^{a_1} p_2^{a_2} \cdots$$

von n ist, also

$$\psi(d) = p^{\alpha-1}(p-\lambda)\cdot p_1^{\alpha_1-1}(p_1-\lambda_1)\cdots$$

oder

$$\frac{\psi(d)}{\lambda^{\alpha}\lambda_1^{\alpha_1}\lambda_2^{\alpha_2}\cdots} = \frac{p^{\alpha-1}(p-\lambda)}{\lambda^{\alpha}}\cdot\frac{p_1^{\alpha_1-1}(p_1-\lambda_1)}{\lambda_1^{\alpha_1}}\cdots,$$

so wird mit Rücksicht darauf, daſs hier, sobald einer der Exponenten $\alpha, \alpha_1, \ldots$ der Null gleich ist, der dem entsprechenden Primfaktor zugehörige Faktor des Ausdruckes durch 1 zu ersetzen ist, die Summe all' dieser Quotienten gleich dem Produkte

$$\left[1 + \frac{p-\lambda}{\lambda} + \frac{p(p-\lambda)}{\lambda^2} + \cdots + \frac{p^{\alpha-1}(p-\lambda)}{\lambda^{\alpha}}\right]\cdot$$
$$\left[1 + \frac{p_1-\lambda_1}{\lambda_1} + \frac{p_1(p_1-\lambda_1)}{\lambda_1^{\,2}} + \cdots + \frac{p_1^{\alpha_1-1}(p_1-\lambda_1)}{\lambda_1^{\alpha_1}}\right]\cdot$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$

sein, in welchem der erste Faktor gleich

$$1 + \frac{p-\lambda}{\lambda}\left(1 + \frac{p}{\lambda} + \cdots + \left(\frac{p}{\lambda}\right)^{\alpha-1}\right) = \left(\frac{p}{\lambda}\right)^{\alpha}$$

und die übrigen entsprechend gleich $\left(\frac{p_1}{\lambda_1}\right)^{\alpha_1}, \left(\frac{p_2}{\lambda_2}\right)^{\alpha_2}, \cdots$ sind. Es ergiebt sich daher folgendes, der Formel (40) analoge Resultat:

$$\sum_d \frac{\psi(d)}{\lambda^{\alpha}\lambda_1^{\alpha_1}\lambda_2^{\alpha_2}\cdots} = \frac{n}{\lambda^{\alpha}\lambda_1^{\alpha_1}\lambda_2^{\alpha_2}\cdots}, \tag{48}$$

welches für die Funktion $\varphi_k(n)$ die besondere Gestalt annimmt:

$$\sum_d \frac{\varphi_k(d)}{k^{\alpha+\alpha_1+\cdots}} = \frac{n}{k^{\alpha+\alpha_1+\cdots}}, \tag{49}$$

wie sie von Schemmel (a. a. O.) gegeben und von Goldschmidt bestätigt worden ist; k ist dabei kleiner zu denken als jeder der Primfaktoren von n.

Über eine andere Verallgemeinerung der Eulerschen Funktion s. K. Vahlen, *Ztschr. f. Math. u. Phys.* 40, 1895, p. 126.

12. Die Formel (35^a) für die Funktion $\varphi(n)$ einer nach (33) in Primfaktoren zerlegten Zahl n kann auch folgendermaſsen geschrieben werden:

$$\varphi(n) = n - \sum\frac{n}{p} + \sum\frac{n}{pp_1} - \sum\frac{n}{pp_1p_2}\cdots, \tag{50}$$

wo die erste Summation auf alle verschiedenen Primfaktoren von n, die zweite auf alle Kombinationen aus zwei, die dritte auf alle Kombinationen aus drei derselben, u. s. w. sich bezieht. So treten uns zum ersten Male die Gruppen von Zahlen:

$$
\begin{array}{ll}
(0) & n \\[4pt]
(\mathrm{I}) & \dfrac{n}{p},\ \dfrac{n}{p_1},\ \dfrac{n}{p_2},\ \ldots \\[4pt]
(\mathrm{II}) & \dfrac{n}{pp_1},\ \dfrac{n}{pp_2},\ \dfrac{n}{p_1p_2},\ \ldots \\[4pt]
(\mathrm{III}) & \dfrac{n}{pp_1p_2},\ \dfrac{n}{pp_1p_3},\ \ldots \\
\ldots & \ldots\ldots\ldots
\end{array}
$$

entgegen, die aus der Zahl n selbst hervorgehen, indem man sie durch jeden ihrer verschiedenen Primfaktoren, durch jedes Produkt von zweien derselben, durch jedes Produkt von dreien derselben, u. s. w. dividiert, eine Gruppierung, zu der man in der Zahlentheorie häufig geführt wird. Hier soll vor allem ein sehr eleganter Satz bewiesen werden, der sich auf sie bezieht. Man denke sich für jede der Zahlen in obiger Gruppierung ihre sämtlichen Teiler gebildet, und fasse alle Teiler der Zahlen der geraden Reihen (0), (II), ..., so oft sie darin sich finden, in einen Komplex A, alle Teiler der Zahlen der ungeraden Reihen (I), (III), ... in einen Komplex B zusammen. Es leuchtet ein, dafs diese Komplexe nur Teiler der Zahl n enthalten. Jener Satz aber sagt aus, dafs jeder Teiler einer von 1 verschiedenen Zahl n — für $n = 1$ kann nämlich eine Gruppierung obiger Art offenbar nicht gedacht werden — ebenso oft im Komplexe A wie im Komplexe B vorkomme, die Zahl n selbst ausgenommen, die selbstverständlich nur im Komplexe A und zwar einmal auftreten wird. Um ihn für irgend einen von n verschiedenen Teiler d zu beweisen, bemerke man, dafs ein solcher nur Primfaktoren von n enthält, mindestens einen derselben aber zu einer geringeren Potenz erhoben, wie n. Man bezeichne diejenigen Primfaktoren von n, für welche letzteres gilt, und deren Anzahl k sei, mit

$$
(51) \qquad \pi', \pi'', \ldots \pi^{(k)}
$$

und bedenke, dafs, wenn n durch einen von diesen Primzahlen verschiedenen Primfaktor p dividiert wird, d nicht Teiler von $\frac{n}{p}$ sein kann, da dieser Quotient den Primfaktor p weniger oft enthält als d. Darnach findet sich d einmal als Teiler der Zahl n selbst; k-mal unter den Teilern der Reihe (I), nämlich als Teiler jeder der Zahlen $\frac{n}{\pi}, \frac{n}{\pi'}, \frac{n}{\pi''}, \cdots$; $\frac{k(k-1)}{1 \cdot 2}$-mal unter den Teilern der Reihe (II), nämlich als Teiler der Zahlen $\frac{p}{\pi\pi'}, \frac{p}{\pi\pi''}, \cdots$; ferner $\frac{k(k-1)(k-2)}{1 \cdot 2 \cdot 3}$-mal unter den Teilern der Zahlen (III), u. s. w. Demnach tritt d in dem Komplexe A

$$
1 + \frac{k(k-1)}{1 \cdot 2} + \frac{k(k-1)(k-2)(k-3)}{1 \cdot 2 \cdot 3 \cdot 4} + \cdots
$$

im Komplexe B

$$\frac{k}{1} + \frac{k(k-1)(k-2)}{1 \cdot 2 \cdot 3} + \cdots$$

mal auf, zwei Anzahlen, deren Unterschied die binomische Entwicklung von $(1-1)^k$ und folglich gleich Null ist, wie der Satz es behauptet.

Insbesondere gilt mithin dieser Satz auch für den Teiler 1; da letzterer aber Teiler von jeder der Zahlen des obigen Schemas ist, so gewinnt man den Zusatz: Die Anzahl der Zahlen (0), (II), ... ist ebenso grofs wie die Anzahl der Zahlen (I), (III), ..., ein Resultat, das auch, wie das vorige, unmittelbar eingesehen werden kann.

Von dem so bewiesenen allgemeinen Satze kann sogleich eine weittragende Anwendung gemacht werden. Besteht nämlich zwischen zwei zahlentheoretischen Funktionen $f(n)$, $\psi(n)$ die Beziehung, dafs für jedes ganzzahlige n und seine sämtlichen Teiler $1, d, d', \ldots n$

$$f(n) = \psi(1) + \psi(d) + \psi(d') + \cdots + \psi(n) \tag{52}$$

ist, so kann die Funktion $\psi(n)$ mittels nachstehender Formel auch umgekehrt durch f-Funktionen ausgedrückt werden:

$$\psi(n) = f(n) - \sum f\left(\frac{n}{p}\right) + \sum f\left(\frac{n}{pp_1}\right) - \sum f\left(\frac{n}{pp_1p_2}\right) + \cdots, \tag{53}$$

wo die Summationen den gleichen Umfang haben, wie in der Formel (50). In der That, ersetzt man in den einzelnen Summen die Funktion f nach der angenommenen Beziehung (52) durch ψ-Funktionen, deren Argumente die Teiler des Argumentes von f sind, so geht die Formel (53) über in die folgende:

$$\psi(n) = \sum_{d:(0)} \psi(d) - \sum_{d:(\mathrm{I})} \psi(d) + \sum_{d:(\mathrm{II})} \psi(d) - \cdots,$$

wo die angedeuteten Summationen sich auf die Teiler der einzelnen Reihen des obigen Schemas beziehen, oder noch einfacher:

$$\psi(n) = \sum_A \psi(d) - \sum_B \psi(d),$$

wenn man die erste Summe auf alle Zahlen d des Komplexes A, die zweite auf alle Zahlen d des Komplexes B erstreckt. Dem Satze zufolge heben sich aber die sämtlichen $\psi(d)$ gegenseitig auf, bis auf das eine, so allein übrig bleibende Glied $\psi(n)$.

Z. B. haben wir durch eine Betrachtung, welche unabhängig vom Ausdrucke der Funktion $\varphi(n)$ nur aus ihrer Bedeutung geschöpft ward, die Beziehung (40) bestätigt, die nur der spezielle Fall der Beziehung (52) ist, welche der Annahme $f(n) = n$, $\psi(n) = \varphi(n)$ entspricht. Demnach liefert die aus (52) gezogene Umkehrung (53)

sofort wieder den Ausdruck der Funktion $\varphi(n)$, wie er in der Formel (50) gegeben worden ist.

13. Aber noch eine andere sehr bemerkenswerte Folgerung soll aus den voraufgehenden Betrachtungen hergeleitet werden. Bezeichne $d_{r,s}$ den gröfsten gemeinsamen Teiler der beiden ganzen Zahlen r, s und setze man

$$(54) \qquad \Delta_{r,n} = d_{r,n} - \sum_{(I)} d_{r,s} + \sum_{(II)} d_{r,s} - \sum_{(III)} d_{r,s} + \cdots,$$

wo die erste Summation auf alle Zahlen s der Reihe (I), die zweite auf alle Zahlen s der Reihe (II), u. s. w. erstreckt werden soll. Es wird behauptet: $\Delta_{r,n}$ sei gleich $\varphi(n)$, so oft r teilbar durch n, gleich Null im entgegengesetzten Falle. Zum Beweise nehme man allgemein an, der gröfste gemeinsame Teiler von r und n sei d, so dafs man

$$n = n_1 d, \quad r = r_1 d$$

setzen und n_1, r_1 als relativ prime Zahlen voraussetzen darf. Nun lassen sich die Primfaktoren, aus denen n besteht, in zwei Kategorien verteilen, in diejenigen — wir nennen sie $p_1, p_1', p_1'', \ldots$ — welche in n_1 aufgehen, gleichviel ob sie zugleich auch in d aufgehen, oder nicht, und in diejenigen — sie mögen $p_2, p_2', \ldots$ heifsen —, welche nur in d aufgehen. Betrachten wir dann irgend eine Zahl aus dem obigen Gruppierungsschema, z. B. die Zahl

$$s = \frac{n}{p_1 p_1' p_1'' \cdot p_2 p_2'},$$

so läfst sich diese in der Form schreiben:

$$s = \frac{n_1}{p_1 p_1' p_1''} \cdot \frac{d}{p_2 p_2'},$$

während zugleich $r = r_1 p_2 p_2' \cdot \frac{d}{p_2 p_2'}$ ist. Hieraus folgt $\frac{d}{p_2 p_2'}$ als gröfster gemeinsamer Teiler von r und s, denn $r_1 p_2 p_2'$ ist prim gegen $\frac{n_1}{p_1 p_1' p_1''}$, da die einzelnen Faktoren r_1, p_2, p_2' prim sind gegen n_1. Demnach wird $\frac{d}{p_2 p_2'}$ der gröfste gemeinsame Teiler von r und jeder derjenigen Zahlen s des Schemas sein, die aus n hervorgehen, wenn mit p_2, p_2', sonst aber nur durch eine Kombination der Primzahlen $p_1, p_1', p_1'', \ldots$ dividiert wird. Solcher Zahlen giebt es offenbar ebensoviele, wie in dem, analog mit dem früheren gebildeten, jetzt aber auf n_1 bezogenen Gruppierungsschema:

$$n_1$$

$$\frac{n_1}{p_1}, \quad \frac{n_1}{p_1'}, \quad \frac{n_1}{p_1''}, \ldots$$

$$\frac{n_1}{p_1 p_1'}, \quad \frac{n_1}{p_1 p_1''}, \quad \frac{n_1}{p_1' p_1''}, \ldots$$

vorhanden sind, und der einer jeden von ihnen entsprechende gröfste gemeinsame Teiler $d_{r,s} = \frac{d}{p_2 p_2'}$ wird in (54), den einzelnen Reihen dieses Schemas entsprechend, mit abwechselnden Vorzeichen genommen sein also sich fortheben, da dem obigen Zusatze gemäfs die Anzahl der Glieder in den geraden Reihen des vorstehenden Schemas gleich der Anzahl derjenigen in den ungeraden Reihen ist, ausgenommen den Fall, dafs die vorige Gruppierung nicht existiert, d. h. den Fall $n_1 = 1$ oder $d = n$, also den Fall, in welchem r teilbar ist durch n. — Während sonst aus dem Gesagten allgemeiner hervorgeht, dafs $\varDelta_{r,n} = 0$ ist, findet sich im letztgenannten Falle, da dann $d = d_{r,n} = n$, also der zuvorbetrachtete gröfste gemeinsame Teiler $d_{r,s} = \frac{d}{p_2 p_2'} = \frac{n}{p_2 p_2'}$, ist, u. s. w., endlich aber die Primzahlen $p_2, p_2', \ldots$ die sämtlichen Primfaktoren von n sind, die Gleichung:

$$\varDelta_{r,n} = n - \sum \frac{n}{p} + \sum \frac{n}{pp_1} + \cdots$$

d. h., wie behauptet ward, $\varDelta_{r,n} = \varphi(n)$.

Aus diesem Satze schliefst man leicht, dafs die Funktion $\varDelta_{r,n}$ mit der **Euler**schen Funktion $\varphi(n)$ die Eigenschaft gemein hat, dafs für ein Produkt $n'n''$ zweier relativ primer Zahlen n', n''

$$\varDelta_{r,n'n''} = \varDelta_{r,n'} \cdot \varDelta_{r,n''} \tag{55}$$

ist. Wenn nämlich r teilbar ist durch $n'n''$, so ist's dies auch einzeln durch n' und durch n'', und die vorige Gleichung geht in die folgende über:

$$\varphi(n'n'') = \varphi(n') \cdot \varphi(n''),$$

welche richtig ist; im entgegengesetzten Falle, in welchem die linke Seite der Gleichung (55) Null sein würde, könnte r nicht durch jede der beiden Zahlen n', n'' zugleich teilbar sein und daher würde mindestens ein Faktor der rechten Seite und so auch die ganze rechte Seite derselben Gleichung verschwinden. Diese aus dem vorigen Satze gefolgerte Beziehung (55) kann auch direkt bewiesen, und dann umgekehrt der Satz aus ihr hergeleitet werden; so geschieht es bei Lucas, *th. d. nombres* Nr. 223.

Mit Hilfe des letzteren aber läfst sich sogleich eine merkwürdige Formel gewinnen, welche von **Stephen Smith** (*Proceed. of the London's Mathem. Society* VII, Mai 1876) gegeben und später von **Mansion** (*Mess. of Math.* (2) 7, 1877; p. 81; *Ann. de la soc. scientifique de Bruxelles* t. II) verallgemeinert worden ist. Man betrachte nämlich die Determinante

$$\begin{vmatrix} d_{1,1}, & d_{1,2}, & d_{1,3}, & \ldots & d_{1,n} \\ d_{2,1}, & d_{2,2}, & d_{2,3}, & \ldots & d_{2,n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ d_{n,1}, & d_{n,2}, & d_{n,3}, & \ldots & d_{n,n} \end{vmatrix}.$$

In der Reihe der Indices $1, 2, 3, \ldots n$ finden sich die sämtlichen Zahlen s, aus denen die Reihen (I), (II), (III), ... des früheren Schemas bestehen, vor; daher kann man nach bekannten Determinantensätzen durch Subtraktion und Addition gewisser Vertikalreihen von resp. zur letzten die Elemente dieser letzten Vertikalreihe durch

$$\Delta_{1,n}, \Delta_{2,n}, \ldots \Delta_{n-1,n}, \Delta_{n,n},$$

welche dem obigen Satze zufolge

$$0, 0, \ldots 0, \varphi(n)$$

gleich sind, ersetzen; demgemäſs wird dann die Determinante gleich $\varphi(n)$-mal der analog gebildeten, nur bis zum Index $n-1$ fortgesetzten Determinante sein. Hieraus erschlieſst man durch Wiederholung derselben Betrachtung diese Formel von Smith:

$$\begin{vmatrix} d_{1,1}, & d_{1,2}, & \ldots & d_{1,n} \\ d_{2,1}, & d_{2,2}, & \ldots & d_{2,n} \\ \cdot & \cdot & \cdot & \cdot \\ d_{n,1}, & d_{n,2}, & \ldots & d_{n,n} \end{vmatrix} = \varphi(1)\,\varphi(2)\ldots\varphi(n). \tag{56}$$

Wie sogleich einleuchtet, kann man mittels derselben die Eulersche Funktion $\varphi(n)$ als Quotienten zweier Determinanten darstellen, welche ausschlieſslich aus gröſsten gemeinsamen Teilern zusammengesetzt sind.

Viertes Kapitel.

Der Euclidische Algorithmus.

1. Die Sätze über die Teilbarkeit der ganzen Zahlen sind im zweiten Kapitel aus dem Begriffe eines Modulus von ganzen Zahlen hergeleitet worden. Von ganz anderer Grundlage aus hat sie Poinsot entwickelt, wobei er nicht notwendiger aber sehr anschaulicher Weise von geometrischer Betrachtung Gebrauch gemacht hat (*Journ. d. Math.* 10, 1845, p. 1); leider involviert seine Darstellung einen Mangel, wodurch sie wie ein fehlerhafter Zirkel erscheint, indem sie sich auf die erst zu erweisende Aussage stützt, das Produkt hm sei durch n nicht teilbar, wenn h prim zu n und $m < n$; aber man kann diesen Mangel ergänzen und so der schönen Poinsotschen Beweismethode volle Giltigkeit verleihen (s. Bachmann, *Elemente d. Zahlenth.* 1892, p. 19). Doch führt auch diese Methode, wie die oben angewendete, auf das fundamentale Prinzip zurück, nach welchem jede ganze Zahl m in Bezug auf eine gegebene (positive) ganze Zahl n in die Gestalt

$$m = qn + r \tag{1}$$

$$(q \text{ ganze Zahl}, \quad 0 \overline{\gtrless} r < n)$$

gesetzt werden kann. Der Versuch liegt daher nahe, unmittelbar auf dieser grundlegenden Eigenschaft selbst die Theorie der Teilbarkeit zu erbauen, und auch dies hat schon Poinsot a. a. O. und später Lejeune-Dirichlet in seinen zahlentheoretischen Vorlesungen (s. dieselben, herausg. v. Dedekind, 4. Aufl. 1894, § 4) gethan.

Setzt man in (1) n_1 statt r, so erhält man

$$m = qn + n_1, \quad 0 \overline{\overline{<}} n_1 < n.$$

Aber nun kann man, an Stelle von n die Zahl n_1, falls sie nicht Null ist, zu Grunde legend, wieder

$$n = q_1 n_1 + n_2, \quad 0 \overline{\overline{<}} n_2 < n_1$$

setzen und so fortfahren:

$$n_1 = q_2 n_2 + n_3, \quad 0 \overline{\overline{<}} n_3 < n_2,$$
$$n_2 = q_3 n_3 + n_4, \quad 0 \overline{\overline{<}} n_4 < n_3,$$
$$\cdots\cdots\cdots\cdots$$

Da hierbei die positiven ganzen Zahlen $n, n_1, n_2, n_3, \ldots$ stets abnehmen, ihre Menge also nur endlich sein kann, mufs man schliefslich auf einen Rest n_{k+1} kommen, welcher Null ist und so den weiteren Fortgang der Entwicklung verhindert. Es entsteht also eine Reihe von Gleichungen:

$$\begin{aligned} m &= qn + n_1, \\ n &= q_1 n_1 + n_2, \\ &\cdots\cdots \\ n_{k-2} &= q_{k-1} n_{k-1} + n_k, \\ n_{k-1} &= q_k n_k, \end{aligned} \tag{2}$$

deren Gesamtheit der Euclidische Algorithmus heifst; die Zahlen $n, n_1, n_2, \ldots n_k$, ebenso die Zahlen $q_1, q_2, \ldots q_k$ sind positiv, q aber kann auch Null oder negativ sein, das erstere, wenn $m > 0$ aber $< n$, das letztere, wenn m negativ ist.

Die Zahl n_k, auf welche der Euclidische Algorithmus führt, ist der gröfste gemeinsame Teiler von m und n. In der That geht n_k zufolge der Gleichungen (2) in n_{k-1}, also wegen der vorletzten dieser Gleichungen auch in n_{k-2} u. s. w., endlich wegen der zweiten dieser Gleichungen in n und wegen der ersten auch in m auf, mithin ist n_k ein gemeinsamer Teiler von m und n; aber jeder gemeinsame Teiler dieser beiden Zahlen geht auch umgekehrt wegen der ersten der Gleichungen (2) in n_1, folglich wegen der zweiten derselben auch in n_2 u. s. w., endlich auch in n_k auf, welche Zahl demnach von allen gemeinsamen Teilern von m, n der gröfste ist und in ihren Teilern zugleich die sämtlichen gemeinsamen Teiler dieser beiden Zahlen liefert. Wir haben so zunächst im Euclidi-

schen Algorithmus eine einfache Methode, um den gröfsten gemeinsamen Teiler zweier Zahlen zu ermitteln, eine Methode, welcher vor der im zweiten Kapitel angegebenen der wesentliche Vorzug zukommt, dafs sie nicht erst der Zerlegung der beiden Zahlen in ihre Primfaktoren bedarf.

Aber dieser Algorithmus führt auch mit Leichtigkeit zum Euclidischen Fundamentalsatze von der Teilbarkeit der ganzen Zahlen. Sei h eine beliebige ganze Zahl; multipliziert man die Gleichungen (2) durchweg mit h, so entstehen die folgenden:

$$\begin{aligned} hm &= qh \cdot n + hn_1, \\ hn &= q_1 \cdot hn_1 + hn_2, \\ &\cdots\cdots \\ hn_{k-1} &= q_k \cdot hn_k, \end{aligned}$$

aus denen man successive schliefst, dafs jeder gemeinsame Teiler von hm und n in $hn_1, hn_2, \cdots hn_k$ enthalten sein und demnach in dem besonderen Falle, wo m, n relativ prim sind, ihr gröfster gemeinsamer Teiler n_k also gleich 1 ist, in h aufgehen mufs (s. Satz VI des 2. Kap.). Ist demnach nicht nur m, sondern auch h relativ prim zu n, so mufs auch das Produkt beider Zahlen es sein (s. Satz VII ebendas.).

2. Wir haben nicht nötig, nun die weiteren Sätze über Teilbarkeit zu wiederholen, wenden uns vielmehr dazu, den Euclidischen Algorithmus an sich näher zu betrachten, wobei wir uns aber durchweg auf den Fall positiver, relativ primer Zahlen m, n beschränken wollen, sodafs der letzte Rest n_k gleich 1 ist. Die sämtlich dann (bis auf die erste, welche auch 0 sein kann) positiven ganzen Zahlen $q, q_1, q_2, \ldots q_k$ sind die gröfsten Ganzen, die in den Brüchen $\frac{m}{n}, \frac{n}{n_1}, \frac{n_1}{n_2}, \cdots \frac{n_{k-1}}{n_k}$ resp. enthalten sind, allgemein:

$$q_i = \left[\frac{n_{i-1}}{n_i}\right].$$

Zunächst erschliefst man unmittelbar aus den Gleichungen (2), indem man ihnen die Form giebt:

$$(2^a) \qquad \begin{aligned} \frac{m}{n} &= q + \frac{n_1}{n}, \\ \frac{n}{n_1} &= q_1 + \frac{n_2}{n_1}, \\ &\cdots\cdots \\ \frac{n_{k-2}}{n_{k-1}} &= q_{k-1} + \frac{n_k}{n_{k-1}}, \\ \frac{n_{k-1}}{n_k} &= q_k, \end{aligned}$$

die Entwicklung des Bruchs $\frac{m}{n}$ in einen (gewöhnlichen) Kettenbruch:

$$\frac{m}{n} = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots + \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}}}. \tag{3}$$

Betrachten wir ferner die folgende Reihe von Gleichungen, in denen h eine der Zahlen $2, 3, \ldots k+1$ bezeichnet:

$$\begin{aligned} x &= qy + y_1, \\ y &= q_1 y_1 + y_2, \\ &\cdots\cdots \\ y_{h-2} &= q_{h-1} y_{h-1} + y_h! \end{aligned} \tag{4}$$

Werden in ihnen y_{h-1}, y_h ganz beliebig als positive ganze Zahlen gewählt, so erhalten offenbar auch $y_{h-2}, y_{h-3}, \cdots y_1, y, x$ zugehörige positive ganzzahlige Werte, die eine wachsende Reihe bilden, sodafs die Gleichungen (4) einen anfänglichen Teil des den Zahlen x, y entsprechenden Euclidischen Algorithmus darstellen; insbesondere werden sie ihn ganz darstellen, wenn $y_h = 0$, und werden x, y relativ prim werden, wenn zugleich $y_{h-1} = 1$ gewählt wird, bei welcher Wahl dann aus den Gleichungen (4) die Entwicklung

$$\frac{x}{y} = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots + \cfrac{1}{q_{h-1}}}} \tag{5}$$

hervorgeht. Es ist leicht, allgemein anzugeben, wie x, y durch die Gröfsen y_h, y_{h-1} bestimmt werden. Unmittelbar entnimmt man aus den Gleichungen (4) den Wert

$$y_{h-2} = q_{h-1} y_{h-1} + y_h. \tag{6}$$

Setzt man diesen in die vorletzte der Gleichungen, nämlich

$$y_{h-3} = q_{h-2} y_{h-2} + y_{h-1}$$

ein, so ergiebt sich weiter

$$y_{h-3} = (q_{h-2} q_{h-1} + 1) y_{h-1} + q_{h-2} y_h. \tag{6^1}$$

Dieser Wert zugleich mit demjenigen von y_{h-2} in die drittletzte der Gleichungen (4)

$$y_{h-4} = q_{h-3} y_{h-3} + y_{h-2}$$

eingesetzt, giebt

$$y_{h-4} = [q_{h-3}(q_{h-2} q_{h-1} + 1) + q_{h-1}] y_{h-1} + (q_{h-3} q_{h-2} + 1) y_h \tag{6^2}$$

u. s. w. Jede der Gröfsen $y_{h-2}, y_{h-3}, y_{h-4}, \cdots y, x$ findet sich somit als eine homogene lineare Funktion von y_{h-1}, y_h ausgedrückt, deren Koeffizienten, weil aus den positiven ganzen Zahlen q_i durch

Additionen und Multiplikationen entstanden, positive ganze Zahlen sein werden. Setzen wir also

$$(7)\qquad \begin{aligned} y &= Y_h y_{h-1} + Y_h' y_h, \\ x &= X_h y_{h-1} + X_h' y_h, \end{aligned}$$

wo wir für h auch noch den Wert 1 zulassen können, wenn wir festsetzen, dafs

$$(7^a)\qquad X_1 = q, \quad X_1' = 1, \quad Y_1 = 1, \quad Y_1' = 0$$

sein soll, so kommt es darauf an, genauer das Gesetz festzustellen, nach welchem die Koeffizienten X_h, Y_h, X_h', Y_h' gebildet sind.

Zunächst sind die Gröfsen X_h, Y_h den Gleichungen (7) zufolge diejenigen Werte von x, y, welche der Annahme $y_{h-1} = 1$, $y_h = 0$ entsprechen; sie haben demnach, wie schon bemerkt, relativ prime Werte und ihr Quotient ist der reduzierte Wert des Kettenbruchs

$$(8)\qquad \frac{X_h}{Y_h} = q + \frac{1}{q_1 +} \cdots + \frac{1}{q_{h-1}}.$$

Läfst man aber von den Gleichungen (4), indem man $h > 1$ voraussetzt, die letzte weg, so gewinnt man aus dem übrigen Systeme derselben zwei, den Gleichungen (7) entsprechende Formeln:

$$\begin{aligned} y &= Y_{h-1} y_{h-2} + Y_{h-1}' y_{h-1}, \\ x &= X_{h-1} y_{h-2} + X_{h-1}' y_{h-1} \end{aligned}$$

mit positiven ganzzahligen Koeffizienten; die Gleichungen (7) andererseits ergeben, wenn für y_h sein Wert aus der letzten der Gleichungen (4) eingesetzt wird,

$$\begin{aligned} y &= Y_h' y_{h-2} + (Y_h - q_{h-1} Y_h') \, y_{h-1}, \\ x &= X_h' y_{h-2} + (X_h - q_{h-1} X_h') \, y_{h-1}, \end{aligned}$$

zwei Formeln, deren Vergleichung mit den eben geschriebenen folgende Beziehungen:

$$(9)\qquad \begin{aligned} X_h' &= X_{h-1}, \quad & X_h &= q_{h-1} X_h' + X_{h-1}', \\ Y_h' &= Y_{h-1}, \quad & Y_h &= q_{h-1} Y_h' + Y_{h-1}' \end{aligned}$$

erkennen läfst; setzt man h, das schon gröfser als 1 anzunehmen war, sogar gröfser als 2 voraus, so gestatten dieselben die anderen zu erschliefsen:

$$(10)\qquad \begin{aligned} X_h &= q_{h-1} X_{h-1} + X_{h-2}, \\ Y_h &= q_{h-1} Y_{h-1} + Y_{h-2}, \end{aligned}$$

welche das Gesetz aussprechen, nach welchem jede der Gröfsen X_h, Y_h aus den zwei voraufgehenden gleichnamigen Gröfsen successive zu

bilden ist, ein Gesetz, das auch noch für den bisher ausgeschlossenen Fall $h = 2$ bestehen bleibt, wenn man übereinkommt,

$$X_0 = 1, \quad Y_0 = 0 \tag{7^b}$$

zu setzen; denn so ergeben sich die Werte

$$X_2 = q_1 q + 1, \quad Y_2 = q_1,$$

welche in der That Zähler und Nenner des reduzierten Kettenbruchs $q + \frac{1}{q_1}$ repräsentieren.

Setzt man $h = k + 1$ in der Formel (8) und vergleicht alsdann mit (3), so findet sich

$$\frac{m}{n} = \frac{X_{k+1}}{Y_{k+1}}.$$

3. Nach dem erhaltenen Bildungsgesetze geht X_h in bestimmter Weise aus den sämtlichen Zahlen $q_{h-1}, q_{h-2}, \ldots q_1, q$ hervor; wir deuten dies mit Gaufs (*Disqu. Ar. art.* 27) durch das Symbol (Gaufsische Klammer)

$$X_h = [q_{h-1}, q_{h-2}, \ldots q_1, q] \tag{11}$$

an. Dem entsprechend wäre zu setzen

$$X_{h-1} = [q_{h-2}, \ldots q_1, q].$$

Offenbar erhält man aber Y_h aus den Zahlen $q_{h-1}, q_{h-2}, \ldots q_1$ genau auf die gleiche Art, wie X_{h-1} aus den Zahlen $q_{h-2}, \ldots q_1, q$, und demgemäfs ist

$$Y_h = [q_{h-1}, q_{h-2}, \ldots q_1] \tag{12}$$

und die Formel (8) nimmt die Gestalt an:

$$\frac{[q_{h-1}, q_{h-2}, \ldots q_1, q]}{[q_{h-1}, q_{h-2}, \ldots q_1]} = q + \frac{1}{q_1 + \cdots + \frac{1}{q_{h-1}}}. \tag{13}$$

Desgleichen erhalten wir die erste der Formeln (10) jetzt in folgender Gestalt:

$$[q_{h-1}, q_{h-2}, \cdots q_1, q] = q_{h-1} \cdot [q_{h-2}, \cdots q_1, q] + [q_{h-3}, \cdots q_1, q]. \tag{14}$$

Eine ähnliche Beziehung aber wird gefunden, wenn man den Gleichungen (7) die folgende dritte hinzufügt:

$$y_1 = Z_h y_{h-1} + Z_h' y_h,$$

welche, wie jene, aus den Formeln (4) sich ergiebt, und wenn man ferner beachtet, dafs offenbar $Z_h = [q_{h-1}, q_{h-2}, \ldots q_2]$ ist. Wählt man nämlich dann wieder $y_{h-1} = 1$, $y_h = 0$, so werden x, y, y_1 resp. identisch mit X_h, Y_h, Z_h und zufolge der ersten der Gleichungen (4) geht die gedachte Beziehung:

$$[q_{h-1}, q_{h-2}, \cdots q_1, q] = q[q_{h-1}, \cdots q_1] + [q_{h-1}, \cdots q_2] \tag{15}$$

hervor. Verbindet man endlich die Formeln (14) und (15) miteinander, so schliefst man ohne Mühe, dafs

(16) $$[q_{h-1}, q_{h-2}, \cdots q_1, q] = [q, q_1, \cdots q_{h-2}, q_{h-1}]$$

ist. In der That, nehmen wir an, diese Gleichheit stünde bereits fest für Gaufsische Klammern von geringerer Gliederanzahl, sodafs wir die Formel (15) auch schreiben können wie folgt:

$$[q_{h-1}, q_{h-2}, \cdots q_1, q] = q[q_1, \cdots q_{h-2}, q_{h-1}] + [q_2, \cdots q_{h-2}, q_{h-1}],$$

so ginge nach dem in der Formel (14) ausgesprochenen Gesetze die rechte Seite dieser Gleichung in $[q, q_1, \cdots q_{h-2}, q_{h-1}]$ über und die Gleichung (16) wäre bewiesen. Da aber für eine nur aus einem oder aus zwei Gliedern bestehende Gaufsische Klammer die Behauptung erfüllt ist — für die erstere selbstverständlich, für die zweite zufolge der Gleichheit

$$[q, q_1] = qq_1 + 1 = [q_1, q]$$

— so gilt der in (16) ausgesprochene Satz allgemein.

4. Nachdem wir diese einfachsten Eigenschaften der Gaufsischen Klammern angemerkt haben, kehren wir zu dem Bildungsgesetze der Gröfsen X_h, Y_h wieder zurück. Aus den Gleichungen (10) erschliefst man zunächst durch Elimination von q_{h-1} für $h = 2, 3, \ldots k+1$ die Beziehung:

$$X_h Y_{h-1} - Y_h X_{h-1} = -(X_{h-1} Y_{h-2} - Y_{h-1} X_{h-2}),$$

aus welcher durch successive Verminderung des Index h die analogen

$$X_{h-1} Y_{h-2} - Y_{h-1} X_{h-2} = -(X_{h-2} Y_{h-3} - Y_{h-2} X_{h-3})$$

u. s. f., endlich

$$X_2 Y_1 - X_1 Y_2 = -(X_1 Y_0 - Y_1 X_0)$$

hervorgehen; durch die Multiplikation dieser Gleichungen kommt

$$X_h Y_{h-1} - Y_h X_{h-1} = (-1)^{h-1} \cdot (X_1 Y_0 - Y_1 X_0)$$

d. i. nach den Werten (7^a) und (7^b) einfacher:

(17) $$X_h Y_{h-1} - Y_h X_{h-1} = (-1)^h.$$

Nun nennt man die reduzierten Werte der Kettenbrüche (8), die man für $h = 2, 3, \cdots k+1$ erhält, also die Brüche $\frac{X_2}{Y_2}, \frac{X_3}{Y_3}, \cdots \frac{X_{k+1}}{Y_{k+1}}$, deren Reihe man noch am Anfange die Brüche

$$\frac{X_0}{Y_0} = \frac{1}{0}, \quad \frac{X_1}{Y_1} = \frac{q}{1}$$

hinzuzufügen pflegt, die successiven Näherungsbrüche für den Kettenbruch (3). Zwischen den Zählern und Nennern zweier aufeinanderfolgender Näherungsbrüche besteht also — nach den eben angegebenen Werten der Brüche $\frac{X_0}{Y_0}, \frac{X_1}{Y_1}$ noch für $h = 1$

giltig — die vorstehende Gleichung (17). Sie führt zugleich zur Erkenntnis des Grundes, aus welchem die genannten Brüche als Näherungsbrüche bezeichnet werden. Bemerkt man nämlich, indem man die Gleichungen (4) mit den h ersten der Gleichungen (2) vergleicht, dafs den Werten $y_{h-1} = n_{h-1}$, $y_h = n_h$ die Werte $x = m$, $y = n$ zugehörig sind, so schliefst man mit Rücksicht auf (9) und (7) das Bestehen der beiden Gleichungen

$$m = X_h n_{h-1} + X_{h-1} n_h,$$
$$n = Y_h n_{h-1} + Y_{h-1} n_h.$$

Demgemäfs läfst sich der Unterschied

$$\frac{m}{n} - \frac{X_h}{Y_h}$$

folgendermafsen schreiben:

$$\frac{X_h n_{h-1} + X_{h-1} n_h}{Y_h n_{h-1} + Y_{h-1} n_h} - \frac{X_h}{Y_h} = \frac{n_h \cdot (X_{h-1} Y_h - X_h Y_{h-1})}{Y_h \cdot (Y_h n_{h-1} + Y_{h-1} n_h)},$$

wegen (17) ist also

$$\frac{m}{n} - \frac{X_h}{Y_h} = \frac{(-1)^{h-1} n_h}{Y_h (Y_h n_{h-1} + Y_{h-1} n_h)} = \frac{(-1)^{h-1} n_h}{n Y_h}. \tag{18}$$

Hiernach ist der Unterschied zwischen $\frac{m}{n}$ und den Brüchen:

$$\frac{X_1}{Y_1}, \frac{X_2}{Y_2}, \ldots \frac{X_k}{Y_k}, \frac{X_{k+1}}{Y_{k+1}} \tag{19}$$

mit ungeradem Index positiv, zwischen $\frac{m}{n}$ und denjenigen mit geradem Index negativ; $\frac{m}{n}$ ist gröfser als jene, kleiner als diese, also immer zwischen je zwei aufeinanderfolgenden Brüchen $\frac{X_h}{Y_h}$, $\frac{X_{h+1}}{Y_{h+1}}$, deren Unterschied wegen (17)

$$\frac{X_h}{Y_h} - \frac{X_{h+1}}{Y_{h+1}} = \frac{(-1)^h}{Y_h Y_{h+1}} \tag{20}$$

ist, enthalten, sodafs, da die Gröfsen Y_h mit wachsendem Index, ihrem Bildungsgesetze gemäfs, zunehmen, also

$$\frac{X_h}{Y_h} - \frac{X_{h+1}}{Y_{h+1}} \quad \text{numerisch} \quad < \frac{1}{Y_h^2} \tag{21}$$

ist, a fortiori

$$\frac{m}{n} - \frac{X_h}{Y_h} \quad \text{numerisch} \quad < \frac{1}{Y_h^2} \tag{22}$$

gefunden wird. Insbesondere ist

$$\frac{m}{n} - \frac{X_{k+1}}{Y_{k+1}} = 0.$$

Aus (20) folgt aber weiter

$$\frac{X_{2g}}{Y_{2g}} - \frac{X_{2g+1}}{Y_{2g+1}} = \frac{1}{Y_{2g}\,Y_{2g+1}},$$

$$\frac{X_{2g+1}}{Y_{2g+1}} - \frac{X_{2g+2}}{Y_{2g+2}} = \frac{-1}{Y_{2g+1}\,Y_{2g+2}},$$

$$\frac{X_{2g+2}}{Y_{2g+2}} - \frac{X_{2g+3}}{Y_{2g+3}} = \frac{1}{Y_{2g+2}\,Y_{2g+3}},$$

folglich

$$\frac{X_{2g}}{Y_{2g}} - \frac{X_{2g+2}}{Y_{2g+2}} = \frac{1}{Y_{2g+1}}\left(\frac{1}{Y_{2g}} - \frac{1}{Y_{2g+2}}\right) > 0,$$

$$\frac{X_{2g+1}}{Y_{2g+1}} - \frac{X_{2g+3}}{Y_{2g+3}} = \frac{-1}{Y_{2g+2}}\left(\frac{1}{Y_{2g+1}} - \frac{1}{Y_{2g+3}}\right) < 0,$$

d. h. die Brüche (19) mit geradem Index bilden eine abnehmende, diejenigen mit ungeradem Index eine wachsende Wertreihe. Endlich führt die Formel (18) zur folgenden Gleichung:

$$\frac{\dfrac{m}{n} - \dfrac{X_h}{Y_h}}{\dfrac{X_{h-1}}{Y_{h-1}} - \dfrac{m}{n}} = \frac{n_h}{n_{h-1}} \cdot \frac{Y_{h-1}}{Y_h},$$

aus welcher, da die beiden Faktoren zur Rechten kleiner als Eins sind, hervorgeht, dafs der Bruch $\frac{X_h}{Y_h}$ näher als $\frac{X_{h-1}}{Y_{h-1}}$ an $\frac{m}{n}$ liegt.

Aus all' diesem ist zu erschliefsen, dafs die Gröfsen (19) mit ungeradem und diejenigen mit geradem Index zwei gegen einander konvergierende Wertreihen bilden, deren erste wächst, die zweite abnimmt und deren korrespondierende Glieder immer den Bruch $\frac{m}{n}$ so zwischen sich fassen, dafs die Gröfsen (19) sich ihm fortwährend nähern, bis die letzte derselben ihm gleich wird. Den Grad der Annäherung bestimmt die Ungleichheit (22).

5. Jeder irreduktible Bruch $\frac{a}{b}$, der **zwischen** zwei aufeinanderfolgenden Näherungsbrüchen $\frac{X_{h-1}}{Y_{h-1}}$, $\frac{X_h}{Y_h}$ liegt, hat einen Nenner $b > Y_h$. Denn, da

$$\frac{a}{b} - \frac{X_{h-1}}{Y_{h-1}} \text{ numerisch } < \frac{X_h}{Y_h} - \frac{X_{h-1}}{Y_{h-1}}$$

d. i. kleiner als $\frac{1}{Y_h Y_{h-1}}$ sein mufs so folgt

$$a Y_{h-1} - b X_{h-1} \text{ numerisch } < \frac{b}{Y_h}$$

und da die linke Seite dieser Ungleichheit eine ganze Zahl, aber von Null verschieden ist, mufs $b > Y_h$ sein.

Aus dieser Bemerkung folgt ferner, dafs jeder Näherungsbruch $\frac{X_h}{Y_h}$ von $\frac{m}{n}$ weniger verschieden ist, als irgend ein anderer irreduktibler Bruch $\frac{a}{b}$, dessen Nenner $b < Y_h$ ist. Denn, unterschiede sich $\frac{a}{b}$ im Gegenteil weniger von $\frac{m}{n}$, als $\frac{X_h}{Y_h}$, so würde $\frac{a}{b}$ auch näher an $\frac{m}{n}$ liegen, wie $\frac{X_{h-1}}{Y_{h-1}}$, und daher gewifs mit $\frac{m}{n}$ zugleich zwischen $\frac{X_{h-1}}{Y_{h-1}}$ und $\frac{X_h}{Y_h}$ enthalten sein, was doch dem eben Bemerkten zufolge bei der Annahme $b < Y_h$ nicht möglich ist.

Weiter erschliefst man aus (17) für $h = k + 1$

$$X_{k+1} Y_k - Y_{k+1} X_k = (-1)^{k+1}. \tag{23}$$

Demgemäfs sind X_{k+1}, Y_{k+1}, wie schon bekannt, relative Primzahlen; da nun auch m, n als zwei solche Zahlen vorausgesetzt sind und $\frac{m}{n} = \frac{X_{k+1}}{Y_{k+1}}$ ist, folgert man die Gleichheiten

$$m = X_{k+1}, \quad n = Y_{k+1}$$

und die Gleichheit (23) nimmt die Gestalt an:

$$m Y_k - n X_k = (-1)^{k+1}$$

und lehrt von Neuem den schon im zweiten Kapitel aus anderer Quelle hergeleiteten Satz:

Sind m, n zwei relativ prime Zahlen, so ist die unbestimmte Gleichung

$$mx + ny = 1$$

oder auch

$$mx - ny = 1 \tag{24}$$

in ganzen Zahlen x, y auflösbar.

Zugleich aber ergiebt sich hier eine solche Auflösung der letzteren Gleichung unmittelbar aus dem für die beiden Zahlen m, n aufstellbaren Euclidischen Algorithmus oder aus dem ihm entsprechenden Kettenbruche für $\frac{m}{n}$, nämlich die Auflösung

$$x = (-1)^{k+1} \cdot Y_k, \quad y = (-1)^{k+1} \cdot X_k. \tag{25}$$

Hiermit ist im Wesentlichen die Methode bezeichnet, nach welcher die unbestimmte Gleichung (24), für welche bereits 1613 von Bachet de Méziriac eine Lösung angegeben worden war, durch Lagrange

(*Mém. de Berlin* 1768) aufgelöst worden ist. Die früher mitgeteilte Lösung entsprang der Theorie der Kongruenzen, aus der auch noch auf eine andere Weise eine solche entnommen werden kann — wir kommen beim Fermat'schen Satze, aus welchem Binet*) sowie Libri eine von Poinsot eleganter gefafste Methode der Lösung (s. dazu auch Cauchy, *exercices d'analyse II,* 1841) entwickelt haben, darauf zurück — aber die praktisch wertvollste von allen bleibt die soeben dargestellte, auf dem Euclidischen Algorithmus beruhende Lösungsart, der wir übrigens bald noch eine andere anreihen wollen.

6. Wir beschliefsen die Reihe der voraufgehenden Betrachtungen mit einer weiteren, gleichfalls bedeutsamen Folgerung, indem wir einmal neben dem Kettenbruche (3), in welchem $q > 0$ angenommen werde, den andern in's Auge fassen:

$$(3^a) \qquad q_k + \cfrac{1}{q_{k-1} + \cdots + \cfrac{1}{q_1 + \cfrac{1}{q}}},$$

dessen einzelne Nenner — die sogenannten Teilnenner — die früheren Nenner einschliefslich des Anfangsgliedes, aber in umgekehrter Reihenfolge sind.

Der Formel (13) entsprechend ist der Kettenbruch (3) gleich dem Quotienten

$$\frac{X_{k+1}}{Y_{k+1}} = \frac{[q_k, q_{k-1}, \cdots q_1, q]}{[q_k, q_{k-1}, \cdots q_1]},$$

aus gleichem Grunde aber wird der Kettenbruch (3ᵃ) zunächst durch den Quotienten

$$\frac{[q, q_1, \cdots q_{k-1}, q_k]}{[q, q_1, \cdots q_{k-1}]}$$

darstellbar sein, für welchen man jedoch mit Rücksicht auf die in (16) ausgesprochene Eigenschaft der Gaufsischen Klammern auch

$$\frac{[q_k, q_{k-1}, \cdots q_1, q]}{[q_{k-1}, \cdots q_1, q]}$$

d. i. $\frac{X_{k+1}}{X_k}$ setzen darf. Demnach werden die zwei Kettenbrüche (3) und (3ᵃ) mit umgekehrter Folge ihrer Glieder dann und nur dann den gleichen Wert haben, wenn

$$(26) \qquad X_k = Y_{k+1}$$

oder, was nach (23) auf dasselbe hinauskommt, wenn

$$(26^a) \qquad \frac{Y_{k+1}^2 + (-1)^{k+1}}{X_{k+1}} = Y_k$$

*) s. *Journal de Math.* 6, p. 450.

ist. Da aber dann $\frac{X_{k+1}}{Y_{k+1}}$ und $\frac{X_{k+1}}{X_k}$ denselben irreduktiblen Bruch darstellen, für welchen der entsprechende gewöhnliche Kettenbruch mittels des Euclidischen Algorithmus eindeutig bestimmt ist, müssen unter der Voraussetzung (26) oder (26ᵃ) die Kettenbrüche (3) und (3ᵃ) mit einander d. h. die Reihe der Teilnenner (einschliefslich des Anfangsgliedes)

$$(27) \qquad q, q_1, q_2, \cdots q_{k-2}, q_{k-1}, q_k$$

mit der umgekehrten Reihe

$$q_k, q_{k-1}, q_{k-2}, \cdots q_2, q_1, q$$

identisch sein; die Reihe der Teilnenner ist dann symmetrisch d. h. zwei gleichweit vom Anfang und vom Ende der Reihe (27) abstehende Zahlen sind einander gleich.

Für einen symmetrisch gebauten Kettenbruch (3) ist infolge der dann stattfindenden Gleichung (26ᵃ) der Umstand erforderlich, dafs

$$\frac{Y_{k+1}^2 + (-1)^{k+1}}{X_{k+1}}$$

d. h. der Bruch $\frac{n^2 \pm 1}{m}$ für passend gewähltes Vorzeichen einer ganzen Zahl gleich sei. Das Stattfinden dieses Umstandes reicht hierfür aber auch aus, sobald $1 < n < m$ ist. Um noch Letzteres zu zeigen, nehme man an, für eine bestimmte Einheit ± 1 sei $\frac{n^2 \pm 1}{m}$ einer ganzen Zahl N gleich, die wegen $n < m$ kleiner als n sein mufs, entwickle dann $\frac{m}{n}$ nach dem Obigen in seinen Kettenbruch (3); da $q_k > 1$ gedacht ist, kann man sich hierbei so einrichten, dafs die Anzahl der Teilnenner nach Belieben gerade oder ungerade wird, indem man erforderlichen Falles den letzten Teilbruch $\frac{1}{q_k}$, einen Schlufsnenner 1 zulassend, durch $\cfrac{1}{(q_k - 1) + \cfrac{1}{1}}$ ersetzt. Somit darf man stets voraussetzen, dafs $(-1)^{k+1}$ der gewählten Einheit gleich also

$$N = \frac{n^2 \pm 1}{m} = \frac{Y_{k+1}^2 + (-1)^{k+1}}{X_{k+1}}$$

werde. Schreibt man diese Gleichheit aber in der Form:

$$X_{k+1} \cdot N - Y_{k+1} \cdot Y_{k+1} = (-1)^{k+1},$$

so giebt ihre Verbindung mit (23) die Gleichung

$$X_{k+1}(N - Y_k) = Y_{k+1}(Y_{k+1} - X_k),$$

aus der sich, da X_{k+1}, Y_{k+1} relativ prime Zahlen sind, $N - Y_k$ durch $Y_{k+1} = n$ teilbar, und da N und Y_k kleiner als n, sich $N = Y_k$ und folglich $X_k = Y_{k+1}$ d. i. die Symmetrie des Kettenbruchs (3) ergiebt.

Aus dem so erhaltenen Resultate fliefst ohne weiteres einer der schönsten Sätze der Zahlentheorie, der Folgendes behauptet: **Eine ganze Zahl, welche die Summe zweier relativ primer Quadratzahlen teilt, ist selbst eine solche Summe.** In der That, nehmen wir an, die Zahl m gehe auf in der Summe $r^2 + s^2$, in welcher r, s ohne gemeinsamen Teiler sind; dann sind gewifs auch m, s relativ prim, denn jede Primzahl p, die ihnen gemeinsam wäre, müfste, da sie mit m zugleich in der Summe $r^2 + s^2$ sowie in dem Summanden s^2 aufgeht, auch aufgehen in r^2 und in r selbst, wäre also r, s gemeinsam, gegen die Voraussetzung. Sind aber m und s relativ prim, so kann man eine Zahl s' (den socius von s) so bestimmen, dafs $ss' \equiv 1 \pmod{m}$ ist. Da nun $r^2 + s^2 \equiv 0 \pmod{m}$ ist, findet sich dann $(rs')^2 + 1 \equiv 0 \pmod{m}$; der kleinste positive Rest von $rs' \pmod{m}$ ist mithin eine zu m prime Zahl $n < m$ von der Beschaffenheit, dafs $\frac{n^2+1}{m}$ einer ganzen Zahl gleich ist. Entwickelt man demnach $\frac{m}{n}$ in einen gewöhnlichen Kettenbruch mit gerader Anzahl $k + 1$ von Gliedern, der Art dafs $(-1)^{k+1} = 1$, so wird dieser Kettenbruch ein symmetrischer also, wenn $k + 1 = 2g$ gesetzt wird von der Form

$$(28) \qquad \frac{m}{n} = q + \cfrac{1}{q_1 + \cdots + \cfrac{1}{q_{g-1} + \cfrac{1}{q_{g-1} + \cdots + \cfrac{1}{q_1 + \cfrac{1}{q}}}}}$$

sein. Hier ist

$$\frac{X_g}{Y_g} = q + \cfrac{1}{q_1 + \cdots + \cfrac{1}{q_{g-1}}},$$

$$\frac{X_g}{X_{g-1}} = q_{g-1} + \cfrac{1}{q_{g-2} + \cdots + \cfrac{1}{q}}$$

und

$$\frac{X_{g+1}}{Y_{g+1}} = \frac{q_{g-1} X_g + X_{g-1}}{q_{g-1} Y_g + Y_{g-1}}.$$

Aus dem letzten dieser Quotienten entsteht aber der ganze Kettenbruch (28), wenn man den Teilnenner q_{g-1} durch $\frac{X_g}{X_{g-1}}$ ersetzt; somit findet man

$$\frac{m}{n} = \frac{X_g^2 + X_{g-1}^2}{X_g Y_g + X_{g-1} Y_{g-1}}$$

und weil Zähler und Nenner des rechts stehenden Bruches zufolge der Gleichheit

$$(X_g^2+X_{g-1}^2)(Y_g^2+Y_{g-1}^2)-(X_gY_g+X_{g-1}Y_{g-1})^2=(X_gY_{g-1}-X_{g-1}Y_g)^2,$$

deren rechte Seite den Wert 1 hat, keinen gemeinsamen Teiler zulassen, mufs

$$m = X_g^2 + X_{g-1}^2$$

sein, wie behauptet.

7. Der Euclidische Algorithmus, so wie wir bisher ihn gefafst haben, läfst sich mannigfach modifizieren, ohne an seinen wesentlichen Eigenschaften Einbufse zu erleiden.

In der fundamentalen Beziehung

$$m = qn + r \tag{29}$$

war bisher der Rest stets positiv und kleiner als n gewählt, wobei dann q das gröfste in $\frac{m}{n}$ enthaltene Ganze d. h.

$$q \overline{\gtrless} \frac{m}{n} < q + 1$$

war. Die Gleichung (29) läfst sich aber auch so schreiben:

$$m = q'n - r', \tag{30}$$

wo $q' = q + 1$, $r' = n - r$ also wieder positiv und kleiner als n ist, und somit kann allgemein gesetzt werden

$$m = kn - \varepsilon_1 \nu_1, \tag{31}$$

wenn unter k eine ganze Zahl, unter ν_1 eine positive ganze Zahl $< n$, und unter ε_1 nach Belieben eine der Einheiten $+1$, -1 verstanden wird. Setzt man nun diese Betrachtung fort, indem man zunächst sie auf n, ν_1 anwendet und

$$n = k_1 \nu_1 - \varepsilon_2 \nu_2$$

setzt, dann wieder

$$\nu_1 = k_2 \nu_2 - \varepsilon_3 \nu_3$$

u. s. f., so erhält man an Stelle des gewöhnlichen Euclidischen Algorithmus ein analog gebildetes System von Gleichungen:

$$\begin{aligned} m &= k\nu - \varepsilon_1 \nu_1, \\ \nu &= k_1 \nu_1 - \varepsilon_2 \nu_2, \\ &\cdots\cdots \\ \nu_{\gamma-2} &= k_{\gamma-1} \nu_{\gamma-1} - \varepsilon_\gamma \nu_\gamma, \\ \nu_{\gamma-1} &= k_\gamma \nu_\gamma, \end{aligned} \tag{32}$$

in denen der Gleichmäfsigkeit der Bezeichnung wegen $n = \nu$ gesetzt ist und die $k, k_1, \ldots, k_{\gamma-1}, k_\gamma$ ganze Zahlen, die $\nu, \nu_1, \nu_2, \ldots \nu_\gamma$ abnehmende positive ganze Zahlen bedeuten, deren letzte wieder der

gröfste gemeinsame Teiler der Zahlen m, n und folglich 1 sein wird, wenn diese, wie es geschehen soll, als relativ prim vorausgesetzt werden; die $\varepsilon_1, \varepsilon_2, \ldots \varepsilon_\gamma$ sind Einheiten, die ganz nach Belieben positiv oder negativ gedacht werden dürfen.*) Z. B. können diese Einheiten ε_i in den einzelnen Gleichungen so gewählt werden, dafs der jedesmalige Rest $\varepsilon_i \nu_i$ der absolut kleinste und somit die entsprechende Zahl ν_i positiv und kleiner als $\frac{1}{2}\nu_{i-1}$ wird. Wie die arithmetischen Folgerungen über die Teilbarkeit der Zahlen auch aus dem modifizierten Euclidischen Algorithmus sich ergeben, so bleiben auch die Gesetze, die für den ursprünglichen festgestellt worden sind, im wesentlichen für den modifizierten bestehen; statt des Kettenbruchs (3) für $\frac{m}{n}$ aber stellt sich aus den Gleichungen (32) der allgemeinere heraus:

(33)
$$\frac{m}{n} = k - \frac{\varepsilon_1}{k_1 - \frac{\varepsilon_2}{k_2 - \cdots - \frac{\varepsilon_\gamma}{k_\gamma}}}.$$

Es ist leicht, die Anzahl aller so für einen gegebenen Bruch $\frac{m}{n}$ möglichen Kettenbruchentwicklungen zu bestimmen (s. Vahlen, *Journ. f. Math.* 115, 1895, p. 221). Nennen wir sie — wobei wir uns auf den Fall eines echten Bruchs $\frac{m}{n}$ beschränken dürfen — $f\left(\frac{m}{n}\right)$, so findet sich zuvörderst aus der Bemerkung, dafs der Bruch $\frac{1}{n}$ aufser sich selbst, der Identität

$$\frac{1}{n} = 1 - \frac{n-1}{n} = 1 - \frac{1}{1 + \frac{1}{n-1}}$$

zufolge, nur diejenigen Entwicklungen haben kann, die sich durch Substitution der Entwicklungen von $\frac{1}{n-1}$ ergeben, die Beziehung

$$f\left(\frac{1}{n}\right) = 1 + f\left(\frac{1}{n-1}\right),$$

welche für jedes $n > 1$ besteht; ähnlich also kommt

$$f\left(\frac{1}{n-1}\right) = 1 + f\left(\frac{1}{n-2}\right),$$

$$\cdots\cdots\cdots\cdots$$

$$f\left(\frac{1}{2}\right) = 1 + f\left(\frac{1}{1}\right) = 1 + 1,$$

*) Nach Lagrange nennt man eine Division *division en dedans (par défaut)* oder *en dehors (par excès)*, jenachdem bei ihr die Einheit ε positiv oder negativ gewählt wird.

Gleichungen, aus deren Verbindung

$$f\left(\frac{1}{n}\right) = n \tag{34}$$

hervorgeht. Allgemeiner aber ist, da $\frac{m}{n}$ entweder nur gleich

$$\frac{1}{\left[\frac{n}{m}\right] + \frac{\varrho}{m}}$$

oder gleich

$$1 - \frac{1}{\left[\frac{n}{n-m}\right] + \frac{\sigma}{n-m}}$$

gesetzt werden kann, wobei ϱ, σ die positiven Reste der bezüglichen Divisionen bedeuten, also kleiner sind als resp. m, $n - m$, offenbar

$$f\left(\frac{m}{n}\right) = f\left(\frac{\varrho}{m}\right) + f\left(\frac{\sigma}{n-m}\right),$$

eine Beziehung, in welcher nun die Glieder zur Rechten auf ähnliche Weise weiter in Summanden zerlegt werden können, bis die Zähler gleich 1 werden; bemerkt man aber, dafs hierbei die Summe aller Nenner unverändert, nämlich gleich n bleiben mufs, so folgert man aus der Formel (34) allgemeiner

$$f\left(\frac{m}{n}\right) = n, \tag{35}$$

d. i. den Satz: Jeder (irreduktible echte) Bruch $\frac{m}{n}$ besitzt n Kettenbruchentwicklungen von der Gestalt (33).

8. Es ist nicht ohne Interesse namentlich in rechnerischer Hinsicht, zu untersuchen, wie lang die verschiedenen möglichen Algorithmen (32) bezw. die ihnen entsprechenden Kettenbrüche (33) sich ausdehnen, welcher von ihnen der kürzeste, welcher der längste ist. Indem wir auf die letzten Fragen bald nachher zurückkommen werden, wollen wir hier zunächst Grenzen angeben, welche jene Ausdehnung niemals überschreiten kann.

Werden die Divisionen des Algorithmus sämtlich so eingerichtet, dafs die Zahlen $\varepsilon_i \nu_i$ die absolut kleinsten Reste bedeuten, also allgemein $\nu_i \overline{\gtrless} \frac{1}{2} \nu_{i-1}$ ist, so ergiebt sich offenbar für die Anzahl $\gamma + 1$ der Gleichungen (32), welche die fragliche Ausdehnung mifst, die Ungleichheit

$$\nu_\gamma \overline{\gtrless} \left(\frac{1}{2}\right)^\gamma \cdot \nu,$$

d. i., wegen $\nu = n$ und $\nu_\gamma = 1$, bei beliebiger Wahl des Logarithmensystems

$$\gamma \cdot \log 2 \overline{\gtrless} \log n$$

oder, wenn Briggische Logarithmen gewählt werden, da $\frac{1}{\log 2} < \frac{10}{3}$ ist, die folgende:

$$\gamma < \frac{10}{3} \log n, \tag{36}$$

welche Binet (*Journ. d. Math.* 6, 1841, p. 449) angegeben hat. Man kann sie noch genauer fassen, wenn man verfährt wie Dupré (ebendas. 11, 1846, p. 41), dessen Verfahren auch für den Fall, in welchem die Divisionen sämtlich nach dem ursprünglichen Euclidischen Algorithmus ausgeführt werden, anwendbar ist.

Um den letztern zuerst zu behandeln, betrachten wir die Gleichungen (2) der Nr. 1 und bemerken, dafs ihnen zufolge offenbar

$$\begin{gathered} n \geqq n_1 + n_2, \quad n_1 \geqq n_2 + n_3, \ \ldots \ n_{k-2} \geqq n_{k-1} + n_k, \\ n_{k-1} \geqq 2 n_k > n_k + n_{k+1}, \quad n_{k+1} = 0 \end{gathered} \tag{37}$$

ist. Hieraus folgt durch successives Substituieren in die erste der Ungleichheiten eine andere von dieser Form

$$\begin{gathered} n \geqq g_i n_i + h_i n_{i+1}, \\ (i = 1, 2, \ldots k), \end{gathered} \tag{38}$$

woraus unter Beachtung der in (37) für n_i angegebenen Grenze zur Ermittlung der Koeffizienten g_i, h_i die Rekursionsformeln

$$\begin{gathered} g_{i+1} = g_i + h_i, \quad h_{i+1} = g_i, \\ (i = 1, 2, \ldots k-1) \end{gathered}$$

und durch deren Verbindung mit einander sich endlich

$$\begin{gathered} g_{i+1} = g_i + g_{i-1}, \quad h_{i+1} = g_i, \\ (i = 2, 3, \ldots k-1) \end{gathered} \tag{39}$$

findet. Die hierdurch nicht bestimmten Anfangswerte erkennt man unmittelbar als

$$g_1 = 1, \quad g_2 = 2, \quad h_1 = h_2 = 1.$$

Von Binet (*Par. C. R.* 17, p. 563) ist gefunden — und es soll später bestätigt werden —, dafs die so definierten Zahlen

$$g_1, g_2, g_3, g_4, \ldots$$

durch die allgemeine Formel

$$g_i = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^{i+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{i+1} \right] \tag{40}$$

gegeben werden; für die gegenwärtige Betrachtung hat man aber nicht nötig, von derselben Gebrauch zu machen. Schreibt man nämlich die Ungleichheit (38) für $i = k - 2$ und benutzt darin die letzte der Ungleichheiten (37), so entsteht die folgende:

$$n \overline{\overline{>}} [2(g_{k-2} + g_{k-3}) + g_{k-2}] n_k$$
$$\overline{\overline{>}} (2g_{k-1} + g_{k-2}) n_k \overline{\overline{>}} (g_{k-1} + g_k) n_k$$

oder, wenn man auch noch

(39[a]) $$g_{k+1} = g_{k-1} + g_k$$

setzt und beachtet, dafs $n_k = 1$ ist, einfacher

(41) $$n \overline{\overline{>}} g_{k+1}.$$

Nun setze man statt der Rekursionsformel (39) die allgemeinere:

(42) $$g_{i+1} = rg_i + g_{i-1}$$
$$(i = 1, 2, \cdots k)$$

voraus, in welcher r eine positive ganze Zahl sei, während $g_0 = 1$, $g_1 = r$ sein soll. Bezeichnet dann w die positive Wurzel

$$w = \frac{r}{2} + \sqrt{\frac{r^2}{4} + 1}$$

der quadratischen Gleichung

(43) $$w^2 = rw + 1$$

oder der Gleichung $w = r + \frac{1}{w}$, d. h. ist w der Wert des unendlichen Kettenbruchs

$$w = r + \cfrac{1}{r + \cfrac{1}{r + \cdots}},$$

sodafs der Formel (42) gemäfs die Brüche

$$\frac{g_1}{g_0}, \quad \frac{g_2}{g_1}, \quad \frac{g_3}{g_2}, \quad \frac{g_4}{g_3}, \cdots$$

die successiven Näherungsbrüche des letzteren sein würden, so schliefst man aus eben derselben Formel

$$g_2 = r^2 \quad + 1 > wr$$
$$g_3 = rg_2 + g_1 > wr^2 \quad + r \quad > w^2 r$$
$$g_4 = rg_3 + g_2 > w^2 r^2 + wr > w^3 r$$

u. s. f., allgemein

(44) $$g_{i+1} > w^i \cdot r.$$

In dem zuvor erörterten besonderen Falle ist $r = 1$, folglich $w^2 = w + 1$, d. h.

$$w = \frac{1 + \sqrt{5}}{2}$$

und somit

$$g_{i+1} > \left(\frac{1 + \sqrt{5}}{2}\right)^i.$$

Die Formel (41) geht dadurch über in die andere:

$$n > \left(\frac{1 + \sqrt{5}}{2}\right)^k,$$

aus welcher $k < \frac{\log n}{\log \frac{1+\sqrt{5}}{2}}$ oder, wenn z_n die Anzahl der Ziffern ist, aus denen die im dekadischen Systeme geschriebene Zahl n besteht, und Briggische Logarithmen gewählt werden, a fortiori

(45) $$k < \frac{z_n}{\log \frac{1+\sqrt{5}}{2}}.$$

Da $\frac{1}{\log \frac{1+\sqrt{5}}{2}} < 5$ ist, so schliefst man hieraus umsomehr

(45ᵃ) $$k < 5 z_n,$$

wie es Lamé (*Par. C. R.* 19, 1844, p. 867) auf Grund der Formel (40) festgestellt hat.

9. Gehen wir nun zu dem modifizierten Euclidischen Algorithmus (32) wieder zurück, bei welchem jetzt die Divisionen so ausgeführt gedacht werden mögen, dafs der jedesmalige Rest $\varepsilon_i \nu_i$ der absolut kleinste d. h. $\nu_i < \frac{1}{2}\nu_{i-1}$ ist. Stellt man dann ν_{i-1} in der fundamentalen Form

(46) $$\nu_{i-1} = q\nu_i + \varrho,$$

worin $0 \overline{\overline{<}} \varrho < \nu_i$, dar, so mufs $q \overline{\overline{>}} 2$ sein; ist ferner $\varrho < \frac{1}{2}\nu_i$, so stimmt ϱ mit der dem gewählten Algorithmus entsprechenden Zahl ν_{i+1} überein, im entgegengesetzten Falle folgt, wenn man die voraufgehende Formel in der Gestalt

$$\nu_{i-1} = (q+1)\nu_i - (\nu_i - \varrho)$$

schreibt, $\nu_i - \varrho = \nu_{i+1}$ also $\varrho = \nu_i - \nu_{i+1} > \nu_{i+1}$. Somit ist wegen (46) immer

(47) $$\nu_{i-1} \overline{\overline{>}} 2\nu_i + \nu_{i+1}$$
$$(i = 1, 2, 3, \cdots \gamma),$$

denn diese Ungleichheit besteht nach der letzten der Gleichungen (32) auch noch für $i = \gamma$, da $\nu_{\gamma+1}$ als Null anzusehen ist. Vermittelst dieser Ungleichheiten schliefst man nun wieder die folgende für ν:

(48) $$\nu \overline{\overline{>}} g_i \nu_i + h_i \nu_{i+1},$$

die sogleich zu den Rekursionsformeln

$$g_{i+1} = 2g_i + h_i, \quad h_{i+1} = g_i$$
$$(i = 1, 2, 3, \cdots \gamma - 1)$$

und endlich zu dieser:

(49) $$g_{i+1} = 2g_i + g_{i-1}$$
$$(i = 2, 3, \cdots \gamma - 1)$$

hinführt; die hierdurch nicht bestimmten anfänglichen Werte findet man unmittelbar als die folgenden:

$$g_1 = 2, \quad g_2 = 5, \quad h_1 = 1, \quad h_2 = 2$$

und, fügt man noch die Bestimmung $g_0 = 1$ hinzu, so besteht die Formel (49) auch noch für $i = 1$. An späterer Stelle soll gezeigt werden, dafs die so definierten Zahlen g_i durch die allgemeine Formel

$$(50) \qquad g_i = \frac{(1+\sqrt{2})^{i+1} - (1-\sqrt{2})^{i+1}}{2\sqrt{2}}$$

gegeben werden, doch ist diese Bestimmung für die gegenwärtige Betrachtung wieder nicht erforderlich. Man schliefst vielmehr aus (48) für $i = \gamma$

$$\nu \geqq g_\gamma \nu_\gamma \geqq g_\gamma$$

und aus der voraufgeschickten allgemeinen Erörterung für den hier vorliegenden Wert $r = 2$, welchem der Wert $w = 1 + \sqrt{2}$ entspricht,

$$g_\gamma > 2 \cdot (1+\sqrt{2})^{\gamma-1}.$$

Mithin ist umsomehr

$$\nu > 2 \cdot (1+\sqrt{2})^{\gamma-1},$$

und folglich bei dem jetzt betrachteten Algorithmus die Anzahl der erforderlichen Divisionen

$$\gamma < \frac{\log \nu}{\log(1+\sqrt{2})} + \frac{\log \frac{1}{2}(1+\sqrt{2})}{\log(1+\sqrt{2})}$$

oder auch

$$(51) \qquad \gamma < 2{,}6125 \cdot z_n + 0{,}2136,$$

eine Grenze, welche enger ist, als die von Binet angegebene, in (36) ausgesprochene Bestimmung, und der gemäfs die Ausdehnung des modifizierten Euclidischen Algorithmus, wie die Vergleichung mit (45^a) ausweist, für sehr viel geringer als die des gewöhnlichen vermutet werden darf.

Dupré hat seine Betrachtungen mit Modifikationen des Euclidischen Algorithmus beschlossen, welche die Anzahl der erforderlichen Divisionen noch zu verringern geeignet sind. Doch bieten dieselben theoretisch kein besonderes Interesse dar und dürften auch praktisch nicht von Bedeutung sein. Es genüge daher, hier darauf zu verweisen; dagegen soll nicht versäumt werden, noch eine von Binet (a. a. O.) angegebene Modifikation mitzuteilen, welche von gröfserem Interesse ist.

10. Setzt man wieder bei gleicher Bedeutung der Buchstaben wie in (32)

$$m = k\nu - \varepsilon_1 \nu_1,$$

worin also ν_1 positiv und kleiner als ν ist, behält aber nun bei den weiteren Divisionen immer m als Dividenden bei, sodafs zunächst

$$m = k_1 \nu_1 - \varepsilon_2 \nu_2$$

wird, wo die — von der früher so bezeichneten unterschiedene — Zahl ν_2 positiv und kleiner als ν_1 gedacht ist, u. s. f., so erhält man ein endliches System von Gleichungen von der Form:

$$(52) \quad \begin{aligned} m &= k\nu - \varepsilon_1 \nu_1 \\ m &= k_1 \nu_1 - \varepsilon_2 \nu_2 \\ m &= k_2 \nu_2 - \varepsilon_3 \nu_3 \\ &\cdot \;\cdot \;\cdot \;\cdot \;\cdot \;\cdot \;\cdot \\ m &= k_{\gamma-1} \nu_{\gamma-1} - \varepsilon_\gamma \nu_\gamma \\ m &= k_\gamma \nu_\gamma, \end{aligned}$$

in welchem die ε_i nach Belieben positiv oder negativ gewählte Einheiten, die ν_i positive abnehmende ganze Zahlen und auch die k_i ganze Zahlen bedeuten. Auch bei diesem Algorithmus wird jeder gemeinsame Teiler von m und von $n = \nu$ auch in ν_γ aufgehen, doch braucht diese Zahl, obschon der letzten Gleichung zufolge ein Teiler von m, nicht auch in n aufzugehen und wird mithin nicht immer den gröfsten gemeinsamen Teiler von m, n ausmachen. Dagegen bleibt, wie unmittelbar einzusehen, die Formel (36) in Giltigkeit, so oft man bei den Divisionen durchweg die Einheit ε_i so wählt, dafs der jedesmalige Rest der absolut kleinste d. i. $\nu_i < \frac{1}{2} \nu_{i-1}$ wird. Die Gesetze, welche im übrigen der Algorithmus befolgt, sind, obwohl abweichend von denjenigen des Euclidischen, doch ähnlich, und sollen hier in ihren interessantesten Punkten für den Fall verfolgt werden, wo die Einheiten ε_i sämtlich gleich $+1$ gewählt sind.

Bei solcher Wahl schliefst man leicht aus den ersten i der Gleichungen (52) durch Elimination der Zahlen $\nu_1, \nu_2, \ldots \nu_{i-1}$ die Beziehung:

$$(53) \quad m(1 + k_{i-1} + k_{i-1}k_{i-2} + \cdots + k_{i-1}k_{i-2}\cdots k_1) = n \cdot k_{i-1}k_{i-2}\cdots k_1 k - \nu_i,$$

insbesondere also für $i = \gamma$:

$$(54) \quad m(1 + k_{\gamma-1} + k_{\gamma-1}k_{\gamma-2} + \cdots + k_{\gamma-1}k_{\gamma-2}\cdots k_1) = n \cdot k_{\gamma-1}k_{\gamma-2}\cdots k_1 k - \nu_\gamma.$$

Desgleichen findet sich, wenn man von der $i + 1^{\text{ten}}$ der Gleichungen (52) bis zur vorletzten fortgeht, um die Zahlen $\nu_{i+1}, \nu_{i+2}, \ldots \nu_{\gamma-1}$ zu eliminieren, die Gleichung

$$(55) \quad m(1 + k_{\gamma-1} + k_{\gamma-1}k_{\gamma-2} + \cdots + k_{\gamma-1}k_{\gamma-2}\cdots k_{i+1}) = \nu_i \cdot k_i k_{i+1}\cdots k_{\gamma-1} - \nu_\gamma,$$

aus welcher die vorige durch die Annahme $i = 0$ als besonderer Fall wieder hervorgeht. Fafst man diese Gleichung als eine Kongruenz

nach dem Modulus m und setzt successive $i = 0, 1, 2, \cdots \gamma - 1$, so liefert sie das bemerkenswerte Resultat, dafs die sämtlichen Produkte

$$\begin{array}{r} \nu \cdot k k_1 k_2 \cdots k_{\gamma-1} \\ \nu_1 \cdot k_1 k_2 \cdots k_{\gamma-1} \\ \nu_2 \cdot k_2 \cdots k_{\gamma-1} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \nu_{\gamma-1} \cdot k_{\gamma-1} \end{array}$$

(mod. m) einander kongruent sind und die Zahl ν_γ zum gemeinsamen kleinsten positiven Rest haben.

Noch eine andere interessante Folgerung zieht man aus den erhaltenen Formeln. Beachtet man nämlich, dafs nach der letzten der Gleichungen (52)

$$m = k_\gamma \cdot \nu_\gamma \tag{56}$$

ist, so geht aus (54) durch Division mit m sowie mit dem Faktor von n die folgende Formel hervor:

$$\frac{n}{m} = \frac{1}{k k_1 \cdots k_\gamma} + \frac{1}{k k_1 \cdots k_{\gamma-1}} + \frac{1}{k k_1 \cdots k_{\gamma-2}} + \cdots + \frac{1}{k}. \tag{57}$$

Hierbei ist zu bemerken, dafs die Division mit dem Faktor von n jedenfalls erlaubt ist, wenn die Zahlen $k, k_1, \ldots k_{\gamma-1}$ von Null verschieden sind; das ist aber der Fall, wenn $m > n = \nu$ und folglich auch $m > \nu_i$ ist. So ergiebt sich die Möglichkeit, einen beliebigen positiven echten Bruch als Summe von Brüchen darzustellen, welche sämtlich die Einheit zum Zähler haben, ein Satz, der bereits von Lambert (s. dazu Lagrange, *Journ. de l'Ec. polyt. cahier* 5) gegeben worden ist.*)

Die Gleichung (54) lehrt ferner, wie der Binetsche Algorithmus gerade wie der Euclidische zur Aufsuchung des gröfsten gemeinsamen Teilers der Zahlen m, n zu nutzen ist. Aus dieser Gleichung bestätigt sich nämlich zunächst, was schon bemerkt worden, dafs jeder, also auch der gröfste gemeinsame Teiler von m, n in ν_γ aufgehen mufs; obwohl aber nach (56) auch umgekehrt diese Zahl in m aufgeht, braucht doch ν_γ, wie (54) sofort erkennen läfst, nicht auch zugleich in n enthalten zu sein, wird dagegen, wenn dies der Fall ist, gewifs mit dem gröfsten gemeinsamen Teiler d von m, n identisch sein. Um im entgegengesetzten Falle den letzteren zu finden, braucht man jetzt nur mit den Zahlen n, ν_γ so zu verfahren, wie wir im Binetschen Algorithmus mit m, n verfahren sind; dabei wird ein ge-

*) Übrigens finden sich Zerlegungen echter Brüche in solche „Stammbrüche" schon viel früher, selbst schon in dem ältesten Rechenbuche des Ahmes (s. Einleitung).

wisser Rest $\varrho_{\gamma'}$ eingeführt werden, der ein Teiler von n und, falls er auch in ν_γ aufgeht, der gröfste gemeinsame Teiler von n und ν_γ sein wird; entgegengesetzten Falles aber wendet man von neuem den Binetschen Algorithmus auf $\nu_\gamma, \varrho_{\gamma'}$ an und gelangt zu einem Reste $\sigma_{\gamma''}$, der in ν_γ enthalten und, falls er auch in $\varrho_{\gamma'}$ aufgeht, der gröfste gemeinsame Teiler von $\nu_\gamma, \varrho_{\gamma'}$ ist; u. s. w. Dieser Fortgang kann aber nur ein endlicher sein, da die Zahlen $n, \nu_\gamma, \varrho_{\gamma'}, \sigma_{\gamma''}, \ldots$ abnehmende ganze Zahlen sind. Gesetzt also, $\sigma_{\gamma''}$ fände sich als gröfster gemeinsamer Teiler von $\nu_\gamma, \varrho_{\gamma'}$. Diese Zahl geht, weil in ν_γ und $\varrho_{\gamma'}$, auch zugleich in ν_γ und n, und folglich auch zugleich in m und n auf, da $\varrho_{\gamma'}$ (analog mit Gleichung (56)) in n, und ν_γ (wegen (56)) in m enthalten ist; $\sigma_{\gamma''}$ ist demnach ein Teiler von d. Umgekehrt geht d in m, n und folglich zugleich in n und ν_γ, mithin auch in $\varrho_{\gamma'}$ also zugleich in $\nu_\gamma, \varrho_{\gamma'}$, mithin auch in $\sigma_{\gamma''}$ auf. Hieraus findet sich endlich $\sigma_{\gamma''} = d$ d. h. die Binetsche Methode hat uns den gröfsten gemeinsamen Teiler von m, n geliefert.

Dafs diese Methode im Falle relativ primer m, n auch zur Auflösung der unbestimmten Gleichung $mx - ny = 1$ verwandt werden kann, leuchtet aus der Formel (54) und diesen Bemerkungen schon ausreichend ein, doch soll der Leser mit Bezug auf diese Anwendung noch ausdrücklich auf Binets Arbeit verwiesen werden, in welcher sie ausführlich entwickelt wird.

11. Der Euclidische Algorithmus hat zu der Erkenntnis geführt, dafs man sich einem gegebenen Bruche $\frac{m}{n}$ durch eine Reihe von Brüchen fortdauernd anzunähern vermag und zwar in der Weise, dafs ihm kein anderer Bruch mit kleinerem Nenner als der des jedesmaligen Näherungsbruches noch näher anliegen kann. Diese so mehr zufällig gewonnene Erkenntnis läfst sich vertiefen, wenn man geradeswegs die Annäherung untersucht, die bei einem gegebenen Werte w mittels aller Brüche, deren Nenner eine Zahl n nicht übersteigen, erreicht werden kann. (S. hierzu vornehmlich A. Hurwitz, *Math. Ann.* 44, 1894, p. 417, ferner K. Th. Vahlen, am oben angeführten Orte.)

Man denke sich alle irreduktibeln Brüche $\frac{x}{y}$, bei denen x, y numerisch nicht gröfser sind als n, ihrer algebraischen Gröfse nach angeordnet. Die so erhaltene Reihe von Brüchen heifse die **Fareysche Reihe** n^{ter} **Ordnung**. Je nach dem Werte von n erhält man so verschiedene Reihen; doch ist klar, dafs jede folgende Reihe alle Glieder der vorangehenden, die Fareysche Reihe $n + 1^{\text{ter}}$ Ordnung alle Glieder der Fareyschen Reihe n^{ter} Ordnung in sich enthält. Den ersten Werten $n = 1, 2, 3, \cdots$ entsprechend stellen sich folgende Reihen von Brüchen heraus, deren erster und letzter immer statt der Zeichen $-\infty, +\infty$ resp. zu nehmen ist:

$n = 1$: $$-\frac{1}{0}, -\frac{1}{1}, \frac{0}{1}, \frac{1}{1}, \frac{1}{0}$$

$n = 2$: $$-\frac{1}{0}, -\frac{2}{1}, -\frac{1}{1}, -\frac{1}{2}, \frac{0}{1}, \frac{1}{2}, \frac{1}{1}, \frac{2}{1}, \frac{1}{0}$$

$n = 3$: $$-\frac{1}{0}, -\frac{3}{1}, -\frac{2}{1}, -\frac{3}{2}, -\frac{1}{1}, -\frac{2}{3}, -\frac{1}{2}, -\frac{1}{3}, \frac{0}{1}, \frac{1}{3},$$
$$\frac{1}{2}, \frac{2}{3}, \frac{1}{1}, \frac{3}{2}, \frac{2}{1}, \frac{3}{1}, \frac{1}{0}$$

u. s. w. Als anfängliche oder 0te Reihe wollen wir ihnen die Reihe

$$-\frac{1}{0}, \frac{0}{1}, \frac{1}{0}$$

voranstellen. Man sieht sofort, daſs man, um die Fareyschen Reihen zu bilden, nur ihre positiven Glieder zu ermitteln hat, da den letzteren bis auf das Vorzeichen die negativen gleich sind; man könnte sich sogar — doch wollen wir davon abstehen — darauf beschränken, nur diejenigen positiven Glieder zu bilden, welche zwischen $\frac{0}{1}$ und $\frac{1}{1}$ enthalten, also echte Brüche sind, denn die übrigen positiven Glieder entstehen aus jenen durch Umkehrung. Indem wir hinfort nur die Hälfte der Fareyschen Reihen in Betracht ziehen, wollen wir vor allem zeigen, wie die $n+1^{\text{te}}$ Reihe aus der n^{ten} hervorgeht.

Zu diesem Zwecke seien $\frac{r'}{u'}$ und $\frac{s'}{v'}$ zwei beliebige Brüche mit positiven Zählern und Nennern und $\frac{r}{u}$ ein zwischen ihnen enthaltener Bruch. Da hiernach, wenn $\frac{s'}{v'} > \frac{r'}{u'}$ gedacht wird, die Differenzen $\frac{r}{u} - \frac{r'}{u'}$, $\frac{s'}{v'} - \frac{r}{u}$ positiv sind, so sind

$$ru' - ur' = \lambda, \quad us' - rv' = \mu \tag{58}$$

positive ganze Zahlen, und man schlieſst aus ihren Ausdrücken, wenn

$$u's' - r'v' = \Delta \tag{59}$$

gesetzt wird, umgekehrt

$$\Delta \cdot r = \mu r' + \lambda s', \quad \Delta \cdot u = \mu u' + \lambda v' \tag{60}$$

und, da Δ nach der Voraussetzung positiv also von Null verschieden sein muſs,

$$\frac{r}{u} = \frac{\mu r' + \lambda s'}{\mu u' + \lambda v'}. \tag{61}$$

Jeder zwischen $\frac{r'}{u'}$, $\frac{s'}{v'}$ enthaltene Bruch hat folglich die Gestalt (61), wobei λ, μ positive ganze Zahlen bezeichnen, die als relativ prim angesehen werden dürfen. Da aber für irgend welche Werte λ, μ dieser Art sich aus (61) die Differenzen

$$\frac{s'}{v'} - \frac{r}{u} = \frac{\Delta \cdot \mu}{v'(\mu u' + \lambda v')}, \quad \frac{r}{u} - \frac{r'}{u'} = \frac{\Delta \cdot \lambda}{u'(\mu u' + \lambda v')}$$

also positiv ergeben, so liegt auch jeder ihnen entsprechende Bruch von der Gestalt (61) zwischen $\frac{r'}{u'}$, $\frac{s'}{v'}$. Wie leicht zu erkennen, geht jeder gemeinsame Teiler von $\mu r' + \lambda s'$, $\mu u' + \lambda v'$ zugleich in $\Delta \cdot \lambda$ und $\Delta \cdot \mu$ also, da λ, μ relativ prim gedacht werden, in Δ auf; wenn also $\Delta = 1$ ist, sind $\mu r' + \lambda s'$, $\mu u' + \lambda v'$ relativ prim, mithin der Bruch von der Gestalt (61) irreduktibel.

Nachdem dies festgestellt worden, denke man sich die positive Hälfte der Fareyschen Reihe n^{ter} Ordnung gebildet und bezeichne mit $\frac{r'}{u'}$, $\frac{s'}{v'}$ irgend zwei aufeinanderfolgende Glieder derselben; auch nehme man an,

$$\Delta = u's' - r'v'$$

sei der Einheit gleich. Wie schon bemerkt worden, gehören die Brüche $\frac{r'}{u'}$, $\frac{s'}{v'}$ auch der folgenden Fareyschen Reihe an, es giebt mithin nur zwei mögliche Fälle: entweder sind jene Brüche auch in der neuen Fareyschen Reihe wieder zwei aufeinanderfolgende Glieder, oder es liegt mindestens noch ein Glied derselben zwischen ihnen und hat also die irreduktible Gestalt:

$$\frac{\mu r' + \lambda s'}{\mu u' + \lambda v'}.$$

Derjenige Bruch von solcher Gestalt, dessen Zähler und Nenner am kleinsten ist, wäre $\frac{r' + s'}{u' + v'}$, und dieser Bruch müfste daher sicher der neuen Fareyschen Reihe angehören; da er aber in der vorhergehenden noch nicht vorhanden war, müfste von seinem Zähler und Nenner mindestens der eine gleich $n + 1$ sein, daher könnte kein weiterer Bruch von der Gestalt (61) der neuen Reihe mehr angehörig sein und folglich wären

$$(62) \qquad \frac{r'}{u'}, \quad \frac{r' + s'}{u' + v'}, \quad \frac{s'}{v'}$$

drei aufeinanderfolgende Brüche derselben.

Man findet hiernach aus der Fareyschen Reihe n^{ter} Ordnung unter der Voraussetzung, dafs für je zwei aufeinanderfolgende Brüche $\frac{r'}{u'}$, $\frac{s'}{v'}$ derselben die Relation

$$u's' - r'v' = 1$$

erfüllt ist, die $n + 1^{\text{te}}$ **Fareysche** Reihe, indem man zwischen je zwei solche Brüche den mittleren Bruch $\frac{r' + s'}{u' + v'}$ einschaltet, so oft weder sein Zähler noch sein Nenner gröfser als $n + 1$ ist.

Da demzufolge entweder $\frac{r'}{u'}, \frac{s'}{v'}$ oder die drei Brüche (62) aufeinanderfolgende Brüche der $n+1^{\text{ten}}$ Fareyschen Reihe sein werden, für welche letzteren, wenn Zähler und Nenner des mittleren Bruches mit r, u bezeichnet werden,

$$ru' - r'u = s'u - v'r = u's' - r'v' = 1$$

gefunden wird, so behält die $n+1^{\text{te}}$ Fareysche Reihe die für die n^{te} vorausgesetzte Eigenschaft bei. Da nun für je zwei aufeinanderfolgende Brüche der anfänglichen Fareyschen Reihe

$$\frac{0}{1}, \frac{1}{1}, \frac{1}{0}$$

diese Eigenschaft thatsächlich besteht, so gilt sie für jede folgende Reihe und man darf den Satz aussprechen, welchen zuerst Cauchy (*Extrait du Bull. de la Soc. philomat., Exerc. de math.* 1, Paris 1827, p. 114) bewiesen hat:

Sind $\frac{r}{u}, \frac{s}{v}$ zwei aufeinanderfolgende positive Glieder einer **Farey**schen Reihe, so ist immer

$$su - rv = 1. \tag{63}$$

Dieser Satz kann nach Hurwitz umgekehrt werden, wie folgt: Zwei positive Brüche $\frac{r}{u}, \frac{s}{v}$, für welche die vorstehende Beziehung (63) stattfindet, stehen in derjenigen **Farey**schen Reihe, in welcher sie zuerst beide vorkommen, nebeneinander. Zunächst leuchtet ein, dafs jeder Bruch $\frac{r}{u}$ in unendlich vielen Fareyschen Reihen auftreten mufs und zwar zuerst in derjenigen, deren Ordnungszahl gleich der gröfseren der beiden Zahlen r, u ist; daher treten die Brüche $\frac{r}{u}, \frac{s}{v}$ zum ersten Mal beide in der n^{ten} Fareyschen Reihe auf, wenn n die gröfste der Zahlen r, u, s, v ist. Wären sie nun nicht aufeinanderfolgende Glieder dieser Reihe, so läge zwischen ihnen mindestens ein Glied derselben, welches, da die Gleichung (63) vorausgesetzt wird, ein irreduktibler Bruch von der Gestalt

$$\frac{\mu r + \lambda s}{\mu u + \lambda v}$$

sein müfste, während doch Zähler oder Nenner des letztern gröfser als n wäre, was in der n^{ten} Fareyschen Reihe nicht sein kann.

Aus dem Satze von Cauchy erschliefst man einen anderen, welchen zuerst Farey (*Phil. Magaz.* (1) 47, 1816, p. 385, s. das. auch 48, 1817, p. 204) durch Beobachtung aus den Goodwynschen Quotiententafeln abstrahiert hat: In allen **Farey**schen Reihen ent-

steht jeder positive Bruch aus den beiden benachbarten $\frac{r}{u}$, $\frac{s}{v}$ nach der Formel

$$\frac{r+s}{u+v}$$

oder, wie es Lucas bezeichnet, durch Mediation, nach Vahlen's weniger bezeichnender Ausdrucksweise durch Komposition. In der That, sind $\frac{r}{u}$, $\frac{x}{y}$, $\frac{s}{v}$ drei aufeinanderfolgende Glieder der Fareyschen Reihe, so hat man nach Cauchy die beiden Gleichungen

$$ux - ry = 1, \quad sy - vx = 1,$$

also $ux - ry = sy - vx$ d. h.

$$\frac{x}{y} = \frac{r+s}{u+v}.$$

12. Nunmehr sei w ein beliebig gegebener positiver Wert und zwar lassen wir hier auch wieder irrationale Werte zu, wie wir sie schon in Nr. 8 und 9 und schon früher gelegentlich in Betracht gezogen haben. Denkt man sich irgend eine, etwa die n^{te} der Fareyschen Reihen, so wird notwendig w, wenn es nicht mit einem Gliede $\frac{r}{u}$ derselben identisch ist, zwischen zwei aufeinanderfolgenden Gliedern $\frac{r}{u}$, $\frac{s}{v}$ gelegen sein. Diese zwei Glieder, von denen im ersteren Falle das eine zwiefältig gewählt werden kann (indem man, wenn $w = \frac{r}{u}$ ist, für $\frac{s}{v}$ sowohl das $\frac{r}{u}$ voraufgehende als das ihm nachfolgende wählen darf), aber auch in diesem Falle völlig bestimmt ist, wenn wir übereinkommen, in ihm für $\frac{s}{v}$ immer das auf $\frac{r}{u}$ folgende Glied zu nehmen, sollen die der n^{ten} Fareyschen Reihe entsprechenden Näherungswerte von w heifsen. Bildet man sie für die successiven Fareyschen Reihen, so erhält man eine Reihe solcher Paare von Näherungswerten:

$$(64) \qquad u^{(1)}, v^{(1)};\ u^{(2)}, v^{(2)};\ u^{(3)}, v^{(3)};\ \ldots,$$

welche endlich oder unendlich sein wird, jenachdem w rational oder irrational ist. Z. B. stellt sich für die Irrationelle $\sqrt{2}$ eine Reihe heraus, deren anfängliche, den ersten elf Fareyschen Reihen entsprechende Glieder die folgenden sind:

$$(65) \quad \frac{0}{1}, \frac{1}{0};\ \frac{1}{1}, \frac{1}{0};\ \frac{1}{1}, \frac{2}{1};\ \frac{1}{1}, \frac{3}{2};\ \frac{4}{3}, \frac{3}{2};\ \frac{7}{5}, \frac{3}{2};\ \frac{7}{5}, \frac{3}{2};\ \frac{7}{5}, \frac{3}{2};$$
$$\frac{7}{5}, \frac{10}{7};\ \frac{7}{5}, \frac{10}{7};\ \frac{7}{5}, \frac{17}{12};\ \ldots$$

Sind aber die der n^{ten} Fareyschen Reihe entsprechenden Näherungswerte $u^{(n)} = \frac{r}{u}$, $v^{(n)} = \frac{s}{v}$, so folgt aus der Art, wie die $n+1^{\text{te}}$ dieser Reihen aus der n^{ten} hervorgeht, dafs entweder $u^{(n+1)}$, $v^{(n+1)}$ beide mit $u^{(n)}$, $v^{(n)}$ resp. übereinstimmen, wenn nämlich $\frac{r}{u}$, $\frac{s}{v}$ auch in der $n+1^{\text{ten}}$ Reihe zwei aufeinanderfolgende Glieder bleiben, oder aber dafs, da andernfalls w entweder zwischen $\frac{r}{u}$, $\frac{r+s}{u+v}$ oder zwischen $\frac{r+s}{u+v}$, $\frac{s}{v}$ enthalten sein mufs, eine der beiden Zahlen $u^{(n+1)}$, $v^{(n+1)}$ mit $\frac{r+s}{u+v}$ identisch, und die andere dann resp. dem Werte $u^{(n)}$, $v^{(n)}$ gleich sein wird. An der obigen Reihe (65) für die Irrationelle $w = \sqrt{2}$ bestätigt sich diese Bemerkung durch den Augenschein. Unterdrückt man nun die Paare, die einem voraufgehenden gleich sind, sowie im ersten von diesem verschiedenen Paare den ihm mit demselben gemeinsamen Bestandteil, bildet man mithin z. B. aus der Reihe (65) die nachstehende andere:

$$\frac{0}{1},\ \frac{1}{1},\ \frac{2}{1},\ \frac{3}{2},\ \frac{4}{3},\ \frac{7}{5},\ \frac{10}{7},\ \frac{17}{12},\ \ldots, \tag{66}$$

so erhält man die einfache Reihe

$$w^{(1)} = \frac{0}{1},\ w^{(2)},\ w^{(3)},\ w^{(4)},\ \ldots, \tag{67}$$

der verschiedenen Näherungswerte der Zahl w, wie sie durch die successiven Fareyschen Reihen geliefert werden, eine Reihe von Brüchen, die, falls nicht w selbst, wenn es nämlich rational ist, sich unter ihnen findet und ihre Reihe abschliefst, die Eigenschaft hat, gegen die Grenze w zu konvergieren. Hierbei werden die Brüche (67) zum Teil gröfser, zum Teil kleiner als w und somit ihre Abweichung von w bald positiv, bald negativ sein. Bezeichnet man mit ε_i das positive oder negative Vorzeichen der Abweichung $w^{(i)} - w$, so stellt sich der Reihe (67) eine andere an die Seite:

$$\varepsilon_1,\ \varepsilon_2,\ \varepsilon_3,\ \varepsilon_4,\ \ldots, \tag{68}$$

welche nach dem Vorgange von Christoffel und Hurwitz*) die Charakteristik der Zahl w heifsen soll.

Im Falle eines irrationalen w wird die Reihe (68) zugleich mit der Reihe (67) unbegrenzt sein und dann jedes der beiden Vorzeichen $+$, $-$ unendlich oft darin vorkommen. In der That, sind $\frac{r}{u}$, $\frac{s}{v}$ eins der Paare von Näherungswerten (64), zwei Brüche also, zwischen

*) Christoffel in *Ann. di Mat.* (2) 15, 1888, p. 253; das Zeichen ε_1, welches dem Näherungswerte $w^{(1)} = \frac{0}{1}$ entspricht, ist, da $w > 0$ angenommen wird, immer das negative Vorzeichen; Hurwitz am oben angegebenen Orte.

denen w enthalten ist, so wird das nächste, von diesem Paare verschiedene Paar in der Reihe (64) entweder $\frac{r}{u}, \frac{r+s}{u+v}$ oder $\frac{r+s}{u+v}, \frac{s}{v}$ sein, jedenfalls wird also der Bruch $\frac{r+s}{u+v}$ das neu eintretende nächste Glied der Reihe (67) und je nach den angegebenen Fällen wird die Abweichung dieses Gliedes von w positiv oder negativ sein. Die Vorzeichen in der Reihe (68) werden demnach nur solange konstant bleiben können, als die Reihe (67) von einem gewissen Gliede an entweder die Form

$$(69)\qquad \frac{r+s}{u+v}, \frac{2r+s}{2u+v}, \frac{3r+s}{3u+v}, \ldots$$

oder die Gestalt

$$(70)\qquad \frac{r+s}{u+v}, \frac{r+2s}{u+2v}, \frac{r+3s}{u+3v}, \ldots$$

hat, was jedoch nicht dauernd sein kann, da der Ausdruck $\frac{hr+s}{hu+v}$ mit wachsendem h sich der Grenze $\frac{r}{u}$, der Ausdruck $\frac{r+hs}{u+hv}$ sich der Grenze $\frac{s}{v}$ unendlich annähert und demnach die Abweichung der Werte (69) von w zuletzt negativ, diejenige der Werte (70) von w schliefslich positiv werden mufs. Somit wechselt notwendig in der Charakteristik einer Irrationellen w das Vorzeichen unendlich oft.

Bedeutet ε das Vorzeichen $+$, η das Vorzeichen $-$, so kann man die Charakteristik in symbolischer Weise folgendermafsen schreiben:

$$(71)\qquad \eta^{q+1}\,\varepsilon^{q_1}\,\eta^{q_2}\,\varepsilon^{q_3}\ldots,$$

wodurch ausgesprochen sein soll, dafs in derselben $q+1$-mal das negative, dann q_1-mal das positive, dann wieder q_2-mal das negative Zeichen u. s. w. folge.

Der Grund zu der Bezeichnung „Charakteristik“ liegt in dem Umstande, dafs dieselbe nicht nur für eine gegebene Gröfse w durch das Obige eindeutig bestimmt ist, sondern auch umgekehrt nur dieser einen Gröfse entspricht. Um noch letzteres zu erkennen, denke man sich die Charakteristik (71) ganz beliebig gegeben; es ist dann leicht, die zugehörige Reihe von Näherungswerten (67) daraus zu ermitteln. In der That, geht man aus von den Brüchen $\frac{r}{u} = \frac{0}{1} = w^{(1)}$ und $\frac{s}{v} = \frac{1}{0}$, welche für jeden positiven Wert w ein erstes Paar von Näherungswerten bilden, so müssen dem kurz zuvor Bemerkten zufolge, da in der Charakteristik (71) genau q negative Vorzeichen auf das, $w^{(1)}$ entsprechende Zeichen $-$ folgen, in der Reihe (67) der Näherungswerte von w zunächst die nachbezeichneten Werte sich finden:

$$w^{(1)} = \frac{r}{u} = \frac{0}{1},\quad w^{(2)} = \frac{r+s}{u+v} = \frac{1}{1},\quad w^{(3)} = \frac{r+2s}{u+2v} = \frac{2}{1}, \cdots w^{(q)} = \frac{r+qs}{u+qv} = \frac{q}{1};$$

der folgende Bruch $\frac{r + (q + 1)s}{u + (q + 1)v} = \frac{q + 1}{1}$ würde schon gröſser als w sein, da nun in der Charakteristik ein positives Vorzeichen folgen soll. Wählt man daher für $\frac{r}{u}$, $\frac{s}{v}$ resp. die Brüche $\frac{r_1}{u_1} = \frac{q}{1}$, $\frac{s_1}{v_1} = \frac{1}{0}$, so folgen in der Reihe (67) jetzt auf den Bruch $\frac{r_1}{u_1}$ die folgenden:

$$w^{(q+1)} = \frac{r_1 + s_1}{u_1 + v_1},\ w^{(q+2)} = \frac{2r_1 + s_1}{2u_1 + v_1}, \ldots,\ w^{(q+q_1)} = \frac{q_1 r_1 + s_1}{q_1 u_1 + v_1} = \frac{q_1 q + 1}{q_1};$$

desgleichen findet sich, indem man nunmehr für $\frac{r}{u}$, $\frac{s}{v}$ resp. die Brüche $\frac{r_2}{u_2} = \frac{q}{1}$, $\frac{s_2}{v_2} = \frac{q_1 q + 1}{q_1}$ wählt, in der Reihe (67) die weitere Folge von Brüchen:

$$w^{(q+q_1+1)} = \frac{r_2 + s_2}{u_2 + v_2},\ w^{(q+q_1+2)} = \frac{r_2 + 2s_2}{u_2 + 2v_2}, \ldots,\ w^{(q+q_1+q_2)} = \frac{r_2 + q_2 s_2}{u_2 + q_2 v_2},$$

u. s. w. So bildet sich also die Reihe (67) in ganz bestimmter Weise aus den Brüchen $\frac{0}{1}$, $\frac{1}{0}$ allein mittels der gegebenen Charakteristik und aus jener wieder die der letztern entsprechende Gröſse w; falls sie irrational ist, als der Grenzwert der Wertreihe (67).

Da hiernach jeder positiven Irrationellen eine ganz bestimmte unendliche Charakteristik zukommt und umgekehrt, so kann man, der Auffassung von Christoffel sich anschlieſsend, das arithmetische Wesen der Irrationellen in dem Systeme der unendlich vielen ganzen Zahlen $q, q_1, q_2, \ldots$ erblicken, welche die Anzahl der abwechselnd negativen und positiven Zeichenfolgen in der Charakteristik angeben, mit andern Worten: man darf die Irrationelle w als den Ausdruck dieser Abzählungen in ihrer Charakteristik betrachten.

13. Besonders interessant ist es nun, daſs die Charakteristik (71) der Gröſse w aufs engste mit der gewöhnlichen Kettenbruchentwicklung der letzteren verbunden ist und daſs somit die angestellte direkte Untersuchung über die Annäherung an w mittels rationaler Brüche auf die frühere Betrachtung der Kettenbrüche wieder zurückführt.

Hierzu bemerke man, daſs die Gröſse w, welcher die Charakteristik (71) entspricht, nach dem in voriger Nr. zuletzt Bemerkten zwischen $\frac{1}{0}$ und $w^{(q)}$, zwischen $w^{(q)}$ und $w^{(q+1)}$ — noch genauer zwischen $w^{(q)}$ und $w^{(q+q_1)}$ — ferner zwischen $w^{(q+q_1)}$ und $w^{(q+q_1+1)}$ — genauer noch zwischen $w^{(q+q_1)}$ und $w^{(q+q_1+q_2)}$ — u. s. w. enthalten ist. Dies läſst sich durch die folgenden Gleichungen ausdrücken:

$$(72)\qquad w = \frac{r_1 w_1 + s_1}{u_1 w_1 + v_1},\quad w = \frac{r_2 + s_2 w_2}{u_2 + v_2 w_2},\quad w = \frac{r_3 w_3 + s_3}{u_3 w_3 + v_3}, \cdots,$$

wenn darin unter $w_1, w_2, w_3, \ldots$ gewisse positive, die Einheit übersteigende Werte verstanden werden. In der That durchläuft der erste dieser Ausdrücke, wenn w_1 von 0 bis 1 wächst, das Intervall $\frac{s_1}{v_1} = \frac{1}{0}$ bis $\frac{r_1 + s_1}{u_1 + v_1} = w^{(q+1)}$, und wenn nun w_1 weiter wächst bis ∞, das fernere Intervall $w^{(q+1)}$ bis $\frac{r_1}{u_1} = w^{(q)}$; ebenso durchläuft der zweite Ausdruck, während w_2 von 0 bis 1 wächst, das Intervall $\frac{r_2}{u_2} = w^{(q)}$ bis $\frac{r_2 + s_2}{u_2 + v_2} = w^{(q+q_1+1)}$, und bei weiterem Wachsen des w_2 bis ∞ das Intervall von $w^{(q+q_1+1)}$ bis $\frac{s_2}{v_2} = w^{(q+q_1)}$; u. s. w.; indem man mithin in jenen Ausdrücken unter $w_1, w_2, w_3, \ldots$ Werte der angegebenen Art versteht, erhalten sie den Wert w. Aus (72) fliefsen aber, wenn man sich der Werte der Zeichen $r_1, s_1, u_1, v_1, r_2, s_2, \ldots$ erinnert, die Formeln:

$$(73) \qquad w = \frac{r_1 w_1 + s_1}{u_1 w_1 + v_1} = q + \frac{1}{w_1};$$

$$\frac{r_1 w_1 + s_1}{u_1 w_1 + v_1} = \frac{r_2 + w_2 s_2}{u_2 + w_2 v_2} = \frac{r_1 + w_2 (q_1 r_1 + s_1)}{u_1 + w_2 (q_1 u_1 + v_1)} = \frac{r_1 \left(q_1 + \frac{1}{w_2}\right) + s_1}{u_1 \left(q_1 + \frac{1}{w_2}\right) + v_1},$$

woraus

$$(73) \qquad w_1 = q_1 + \frac{1}{w_2}$$

hervorgeht; desgleichen

$$\frac{r_2 + s_2 w_2}{u_2 + v_2 w_2} = \frac{r_3 w_3 + s_3}{u_3 w_3 + v_3} = \frac{(r_2 + q_2 s_2) w_3 + s_2}{(u_2 + q_2 v_2) w_3 + v_2} = \frac{r_2 + \left(q_2 + \frac{1}{w_3}\right) s_2}{u_2 + \left(q_2 + \frac{1}{w_3}\right) v_2},$$

woraus sich

$$(73) \qquad w_2 = q_2 + \frac{1}{w_3}$$

ergiebt, u. s. w. Folglich wird schliefslich w gleich dem aus den Exponenten der Charakteristik (71) zusammengesetzten gewöhnlichen Kettenbruche

$$(74) \qquad w = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots}},$$

in welchem die Teilnenner $q, q_1, q_2, \ldots$, da $w_1, w_2 \ldots$, positiv und gröfser als 1 sind, den Gleichungen (73) zufolge die resp. in $w, w_1, w_2, \ldots$ enthaltenen Ganzen sind; q kann Null sein, wenn $w < 1$ ist, ist aber sonst, wie die sämtlichen Teilnenner $q_1, q_2, \ldots$, eine positive ganze Zahl. Der aus der Charakteristik (71) hervorgehende Kettenbruch (74) ist demnach vollkommen derselbe, wie man ihn durch Anwendung des **Euclid**ischen Algorithmus erhalten würde, und aus dem Bildungsgesetze der Näherungswerte $w^{(1)}, w^{(q)}, w^{(q+q_1)}, w^{(q+q_1+q_2)}, \ldots$, ist sofort

zu ersehen, dafs sie nichts anderes sind als seine successiven Näherungsbrüche.

14. Hieraus fliefst noch eine andere beachtenswerte Folgerung. Es ist gezeigt worden, dafs ein- und dieselbe Charakteristik (71) nicht verschiedenen Werten w, W zukommen kann; es fragt sich, in welcher Beziehung zu einander zwei Werte w, W stehen mögen, für welche die Charakteristiken wenigstens von einer bestimmten Stelle an übereinstimmen.

Sei für die Gröfse w, die wir wieder als irrationell voraussetzen, die Charakteristik (71) bekannt; wir geben sie ausführlicher, wie folgt:

$$(71^a) \qquad \eta^{q+1}\varepsilon^{q_1}\eta^{q_2}\ldots\varepsilon^{q_{h-1}}\eta^{q_h}\varepsilon^{q_{h+1}}\ldots$$

und betrachten daneben die Charakteristik

$$(71^b) \qquad \eta^{q_h}\varepsilon^{q_{h+1}}\ldots,$$

welche den unendlichen Schlufsteil der vorigen bildet. Die positive Irrationelle, welche der letzteren entspricht, heifse w'. Dem soeben Bewiesenen zufolge bestehen dann die Kettenbruchentwicklungen

$$w' = (q_h - 1) + \cfrac{1}{q_{h+1} + \cfrac{1}{q_{h+2} + \cdots}},$$

$$w = q + \cfrac{1}{q_1 + \cdots + \cfrac{1}{q_h + \cfrac{1}{q_{h+1} + \cdots}}}.$$

und folglich die Gleichung

$$w = q + \cfrac{1}{q_1 + \cdots + \cfrac{1}{q_{h-1} + \cfrac{1}{w' + \cfrac{1}{1}}}},$$

der man nach den Formeln in Nr. 3, welche, wie leicht zu übersehen, auch dann gelten, wenn die positiven Teilnenner nicht als ganzzahlig vorausgesetzt werden, die Gestalt

$$w = \frac{[1, w', q_{h-1}, \ldots q_1, q]}{[1, w', q_{h-1}, \ldots q_1]},$$

oder auch durch zwiefache Anwendung der Formel (14) daselbst die folgende:

$$(75) \qquad w = \frac{w'[q_{h-1}, \ldots q_1, q] + [q_{h-1}, \ldots q] + [q_{h-2}, \ldots q]}{w'[q_{h-1}, \ldots q_1] + [q_{h-1}, \ldots q_1] + [q_{h-2}, \ldots q_1]}$$

geben kann. Schreibt man dafür einfacher:

$$(75a) \qquad w = \frac{\alpha w' + \beta}{\gamma w' + \delta},$$

so findet sich zwischen den Koeffizienten $\alpha, \beta, \gamma, \delta$ die Beziehung:

$$\alpha\delta - \beta\gamma = [q_{h-1}, \cdots q] \cdot [q_{h-2}, \cdots q_1] - [q_{h-2}, \cdots q] \cdot [q_{h-1}, \cdots q_1]$$

d. i. bei Beibehaltung früherer Bezeichnungen gleich $X_h Y_{h-1} - X_{h-1} Y_h$, also

$$\alpha\delta - \beta\gamma = \pm 1. \tag{76}$$

Hätte nun eine zweite positive Irrationelle W eine Charakteristik, welche von einer bestimmten Stelle an mit derjenigen von w übereinstimmt, so denke man sich den beiden Charakteristiken gemeinsamen Schlufsteil, welcher (71[b]) sei. Ebenso wie zu den Gleichungen (75a) und (76), gelangt man dann zu den folgenden:

$$W = \frac{Aw' + B}{\Gamma w' + \Delta}, \tag{77}$$

$$A\Delta - B\Gamma = \pm 1, \tag{78}$$

in denen A, B, Γ, Δ, wie zuvor $\alpha, \beta, \gamma, \delta$, ganze Zahlen bedeuten. Durch Elimination von w' aus den beiden Gleichungen (75[a]) und (77) folgt alsdann

$$W = \frac{aw + b}{cw + d}, \tag{79}$$

worin

$$a = A\delta - B\gamma, \quad b = -A\beta + B\alpha,$$

$$c = \Gamma\delta - \Delta\gamma, \quad d = -\Gamma\beta + \Delta\alpha$$

und folglich

$$ad - bc = (A\Delta - B\Gamma)(\alpha\delta - \beta\gamma) = \pm 1 \tag{80}$$

ist.

Nehme man umgekehrt an, zwischen den beiden positiven Irrationellen w, W bestehe die Beziehung (79), in welcher a, b, c, d ganze, der Bedingung (80) genügende Zahlen bedeuten. Ist

$$w = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots}}$$

der gewöhnliche Kettenbruch, welcher der Irrationellen w entspricht, den wir auch schreiben können, wie folgt:

$$w = q + \cfrac{1}{q_1 + \cdots + \cfrac{1}{q_{h-1} + \cfrac{1}{w'}}}, \tag{81}$$

wenn wir unter w' seinen unendlichen Schlufsteil

$$w' = \cfrac{1}{q_h + \cfrac{1}{q_{h+1} + \cdots}}$$

verstehen, so sind, unter Beibehaltung der früheren Bezeichnungen $\frac{X_h}{Y_h}, \frac{X_{h-1}}{Y_{h-1}}$, der h^{te} und $(h-1)^{\text{te}}$ Näherungsbruch von w und deren

Unterschied, wenn man h grofs genug wählt, beliebig klein; endlich besteht die Gleichung

$$w = \frac{X_h w' + X_{h-1}}{Y_h w' + Y_{h-1}}.$$

Durch Einsetzen dieses Ausdrucks in die angenommene Gleichung (79) findet sich

$$W = \frac{(aX_h + bY_h)\, w' + aX_{h-1} + bY_{h-1}}{(cX_h + dY_h)\, w' + cX_{h-1} + dY_{h-1}}.$$

Nun ist

$$\frac{aX_h + bY_h}{aX_{h-1} + bY_{h-1}} = \frac{Y_h}{Y_{h-1}} \cdot \frac{\frac{X_h}{Y_h} + \frac{b}{a}}{\frac{X_{h-1}}{Y_{h-1}} + \frac{b}{a}},$$

ein Ausdruck, dessen erster Faktor positiv und gröfser als 1 ist, da die Y_i mit dem Index i wachsen, während der zweite Faktor der positiven Einheit beliebig nahe gebracht werden kann, indem man h grofs d. h. $\frac{X_{h-1}}{Y_{h-1}}$ nahe genug an $\frac{X_h}{Y_h}$ wählt. Dann ist aber der Quotient

$$\frac{aX_h + bY_h}{aX_{h-1} + bY_{h-1}}$$

ein positiver Wert gröfser als 1, der durch den Quotienten $\frac{A}{B}$ zweier positiver ganzer Zahlen ohne gemeinsamen Teiler dargestellt werden kann. In gleicher Weise bezeichnet der Quotient

$$\frac{cX_h + dY_h}{cX_{h-1} + dY_{h-1}}$$

bei hinreichend grofsem h einen positiven Wert $\frac{C}{D} > 1$, wo C, D positive ganze Zahlen ohne gemeinsamen Teiler bedeuten. Da zudem wegen der Beziehung

$$(aX_h + bY_h)(cX_{h-1} + dY_{h-1}) - (aX_{h-1} + bY_{h-1})(cX_h + dY_h)$$
$$= (ad - bc)(X_h Y_{h-1} - Y_h X_{h-1}) = \pm 1$$

jene Quotienten irreduktibel, ihre Zähler und Nenner also den Zahlen A, B, C, D numerisch gleich sind, so giebt es vier positive ganze Zahlen A, B, C, D so beschaffen, dafs

$$A > B, \quad C > D$$

(82)
$$AD - BC = \pm 1$$

und

$$W = \frac{Aw' + B}{Cw' + D}$$

ist.

Nachdem dies festgestellt worden, entwickele man nun den Bruch $\frac{A}{C}$ in seinen gewöhnlichen Kettenbruch

$$\frac{A}{C} = k + \frac{1}{k_1 + \frac{1}{k_2 + \cdots + \frac{1}{k_{g-1}}}},$$

dessen Gliederzahl man, wie früher bemerkt, nach Belieben gerade oder ungerade, also so wählen kann, dafs, wenn $\frac{A'}{C'}$ den vorletzten Näherungsbruch bedeutet, in der Beziehung

$$AC' - A'C = \pm 1$$

dasselbe Vorzeichen statthat, wie in (82). Eine Vergleichung dieser beiden Beziehungen liefert dann

$$B = A' + Az, \quad D = C' + Cz,$$

wo z eine ganze Zahl ist; diese aber mufs Null sein, da B wie A' positiv und kleiner als A, und D wie C' positiv und kleiner als C ist; somit kommt $B = A'$, $D = C'$ und folglich

$$W = \frac{Aw' + A'}{Cw' + C'}$$

d. h. nach dem Bildungsgesetze der Näherungsbrüche

$$W = k + \frac{1}{k_1 + \cdots + \frac{1}{k_{g-1} + \frac{1}{w'}}}.$$

Vergleicht man diese Formel mit der Formel (81), während man den Kettenbruch für w' in sie beide einsetzt, so ist offenbar, dafs die gewöhnlichen Kettenbrüche der zwei Irrationellen w, W ein und denselben unendlichen Schlufsteil haben oder dafs ihre Charakteristiken bis auf einen verschiedenen endlichen Anfangsteil mit einander identisch sind.

Aus den beiden hiermit erhaltenen reziproken Resultaten erschliefst man endlich den folgenden Satz:

Damit die Charakteristiken (oder die gewöhnlichen Kettenbrüche) zweier positiver Irrationellen w, W von einem etwa verschiedenen anfänglichen Teile abgesehen mit einander identisch sind, ist notwendig und hinreichend, dafs für sie die Beziehungen (79) und (80) erfüllt, oder, wie man zu sagen pflegt, dafs w, W zwei „äquivalente Werte“ sind.

15. Wir wollen endlich versuchen, die Näherungswerte einer jetzt wieder als rational vorausgesetzten positiven Gröfse $w = \frac{m}{n}$, von denen wir erkannt haben, dafs sie enge mit dem Euclidischen

Algorithmus für diese Gröfse zusammenhängen, auch mit dem modifizierten Euclidischen Algorithmus in Verbindung zu bringen.

Ausgehend von den beiden Näherungswerten $\frac{0}{1}, \frac{1}{0}$ erhalten wir durch successive Mediation zunächst die folgenden Paare:

$$\frac{0}{1}, \frac{1}{0}; \quad \frac{1}{1}, \frac{1}{0}; \quad \frac{2}{1}, \frac{1}{0}; \quad \frac{3}{1}, \frac{1}{0}; \quad \ldots \quad \frac{q}{1}, \frac{1}{0}; \tag{83}$$

wo q die gröfste in w enthaltene ganze Zahl bedeutet; das folgende so entstehende Paar von Näherungswerten wäre $\frac{q}{1}, \frac{q+1}{1}$; dies dürfen wir auch bezeichnen durch $\frac{k}{1}, \frac{k-\varepsilon_1}{1}$, wenn wir unter ε_1 nach Belieben die positive oder negative Einheit und entsprechend unter k die Zahl $q+1$ oder q, unter ε_1, k also dieselben Zahlen verstehen, welche im modifizierten Euclidischen Algorithmus durch die gleichen Buchstaben bezeichnet worden sind. Demgemäfs setzen wir, indem wir wieder der Gleichmäfsigkeit in der Bezeichnung wegen ν statt n schreiben, die erste Gleichung dieses Algorithmus an:

$$m = k\nu - \varepsilon_1 \nu_1, \tag{84}$$

eine Gleichung, der man auch die Gestalt

$$\frac{m}{n} = \frac{k \cdot \frac{\nu}{\nu_1} - \varepsilon_1}{\frac{\nu}{\nu_1}} = k - \frac{\varepsilon_1}{\left(\frac{\nu}{\nu_1}\right)} \tag{85}$$

geben kann. Nun liefert die weitere Mediation von den Näherungswerten $\frac{k}{1}, \frac{k-\varepsilon_1}{1}$ aus die folgenden Paare:

$$\frac{k}{1}, \frac{k-\varepsilon_1}{1}; \quad \frac{k}{1}, \frac{2k-\varepsilon_1}{2}; \quad \frac{k}{1}, \frac{3k-\varepsilon_1}{3}; \quad \ldots; \quad \frac{k}{1}, \frac{q'k-\varepsilon_1}{q'}, \tag{86}$$

wo q' diejenige bestimmte ganze Zahl ist, für welche w noch zwischen $\frac{k}{1}, \frac{q'k-\varepsilon_1}{q'}$, aber nicht mehr zwischen $\frac{k}{1}, \frac{(q'+1)k-\varepsilon_1}{q'+1}$ liegt, sodafs das nunmehr folgende Paar von Näherungswerten $\frac{q'k-\varepsilon_1}{q'}, \frac{(q'+1)k-\varepsilon_1}{q'+1}$ sein wird. Wählt man wieder ε_2 nach Belieben gleich $+1$ oder gleich -1, und entsprechend $k_1 = q'+1$ oder $k_1 = q'$, so läfst sich dies letztere Paar auch folgendermafsen bezeichnen:

$$\frac{k_1 k - \varepsilon_1}{k_1}, \quad \frac{(k_1 - \varepsilon_2) k - \varepsilon_1}{k_1 - \varepsilon_2}; \tag{87}$$

mithin liegt $w = \frac{m}{n}$ zwischen den Grenzen

$$k - \frac{\varepsilon_1}{k_1}, \quad k - \frac{\varepsilon_1}{k_1 - \varepsilon_2}$$

und $\frac{v}{v_1}$ wegen (85) zwischen den Grenzen k_1 und $k_1 - \varepsilon_2$, sodaſs man die zweite Gleichung des modifizierten Euclidischen Algorithmus:

$$v = k_1 v_1 - \varepsilon_2 v_2 \tag{88}$$

oder auch diese:

$$\frac{v}{v_1} = k_1 - \frac{\varepsilon_2}{\left(\frac{v_1}{v_2}\right)} \tag{89}$$

ansetzen darf. Fährt man aber fort, durch Mediation von den Brüchen (87) aus die weiteren Paare von Näherungswerten für w zu bilden, so findet man zunächst:

$$\frac{k_1 k - \varepsilon_1}{k_1}, \quad \frac{(k_1 - \varepsilon_2) k - \varepsilon_1}{k_1 - \varepsilon_2}; \quad \frac{k_1 k - \varepsilon_1}{k_1}, \quad \frac{(2k_1 - \varepsilon_2) k - 2\varepsilon_1}{2k_1 - \varepsilon_2};$$
$$\ldots; \frac{k_1 k - \varepsilon_1}{k_1}, \quad \frac{(q'' k_1 - \varepsilon_2) k - q'' \varepsilon_1}{q'' k_1 - \varepsilon_2},$$

unter q'' diejenige bestimmte ganze Zahl verstanden, für welche w noch zwischen den letztgenannten Werten, nicht aber mehr zwischen

$$\frac{k_1 k - \varepsilon_1}{k_1}, \quad \frac{((q'' + 1) k_1 - \varepsilon_2) k - (q'' + 1) \varepsilon_1}{(q'' + 1) k_1 - \varepsilon_2}$$

enthalten ist. Das nächste Paar von Näherungswerten wäre folglich, wenn $\varepsilon_3 = +1$ oder -1, und dementsprechend k_2 gleich $q'' + 1$ oder q'' ist, das Paar

$$\frac{(k_2 k_1 - \varepsilon_2) k - \varepsilon_1 k_2}{k_2 k_1 - \varepsilon_2}, \quad \frac{[(k_2 - \varepsilon_3) k_1 - \varepsilon_2] k - (k_2 - \varepsilon_3) \varepsilon_1}{(k_2 - \varepsilon_3) k_1 - \varepsilon_2};$$

mithin liegt w zwischen den Grenzen

$$k - \frac{\varepsilon_1 k_2}{k_2 k_1 - \varepsilon_2} = k - \frac{\varepsilon_1}{k_1 - \frac{\varepsilon_2}{k_2}}$$

und

$$k - \frac{\varepsilon_1 (k_2 - \varepsilon_3)}{(k_2 - \varepsilon_3) k_1 - \varepsilon_2} = k - \frac{\varepsilon_1}{k_1 - \frac{\varepsilon_2}{k_2 - \varepsilon_3}},$$

und $\frac{v_1}{v_2}$ den Formeln (85) und (89) zufolge zwischen k_2 und $k_2 - \varepsilon_3$, sodaſs man die dritte Gleichung des modifizierten Euclidischen Algorithmus:

$$v_1 = k_2 v_2 - \varepsilon_3 v_3 \tag{89}$$

ansetzen kann; u. s. w. fort.

Man sieht auf solche Weise, wie die successiven Näherungswerte für w bei gehöriger Wahl der Zahlen $k, k_1, k_2, \ldots$, nämlich die Folge der Brüche:

$$(90)\begin{cases} \frac{1}{1}, \frac{2}{1}, \frac{3}{1}, \ldots \frac{k}{1}, {}^{*)} \\ \frac{k-\varepsilon_1}{1}, \frac{2k-\varepsilon_1}{2}, \frac{3k-\varepsilon_1}{3}, \ldots \frac{k_1 k-\varepsilon_1}{k_1}, \\ \frac{(k_1-\varepsilon_2)k-\varepsilon_1}{k_1-\varepsilon_2}, \frac{(2k_1-\varepsilon_2)k-2\varepsilon_1}{2k_1-\varepsilon_2}, \ldots \frac{(k_2 k_1-\varepsilon_2)k-k_2\varepsilon_1}{k_2 k_1-\varepsilon_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

genau zu der Kettenbruchentwicklung führt, die in Nr. 7 für $\frac{m}{n}$ aufgestellt worden ist. Offenbar erhält man aber die erste Reihe der vorstehenden Näherungswerte aus dem Ausdrucke x, wenn man x die Werte $1, 2, 3, \ldots k$ durchlaufen läfst, die zweite aus dem Ausdrucke $k - \frac{\varepsilon_1}{x_1}$, wenn x_1 die Werte $1, 2, 3, \ldots k_1$, die dritte aus dem Ausdrucke $k - \cfrac{\varepsilon_1}{k_1 - \frac{\varepsilon_2}{x_2}}$, wenn x_2 die Werte $1, 2, 3, \ldots k_2$ durchläuft, u. s. w. Wäre hierbei eine der Einheiten ε_i, etwa ε_2, gleich 1, so wäre der Ausdruck

$$k - \cfrac{\varepsilon_1}{k_1 - \frac{\varepsilon_2}{x_2}}$$

für $x_2 = 1$ mit $k - \frac{\varepsilon_1}{k_1 - 1}$ identisch, würde also bereits einmal als vorletztes Glied der vorhergehenden Reihe erhalten sein. Beachtet man dies, so gestattet unsere Betrachtung den folgenden Satz (s. bei Vahlen a. a. O. p. 226) auszusprechen:

In jeder der in Nr. 7 für eine positive rationale Zahl $\frac{m}{n}$ als möglich aufgestellten Kettenbruchentwicklungen:

$$\frac{m}{n} = k - \cfrac{\varepsilon_1}{k_1 - \cfrac{\varepsilon_2}{k_2 - \cdots - \cfrac{\varepsilon_\gamma}{k_\gamma}}}$$

ist die Summe der Teilnenner (einschliefslich des Anfangsgliedes):

$$k + k_1 + k_2 + \cdots + k_\gamma,$$

vermindert um die Anzahl der Einheiten ε_i, welche positiv sind, die gleiche, nämlich ebenso grofs wie die Anzahl aller (positiven endlichen) Näherungswerte der Zahl $\frac{m}{n}$.

---

*) Ist $\frac{m}{n}$ ein echter Bruch, also $q = 0$, so fällt diese erste Reihe ganz fort oder reduziert sich auf das einzige Glied $\frac{1}{1}$, jenachdem man $k = q$ oder $k = q + 1$ wählt.

Wählt man z. B. $\frac{m}{n} = \frac{237}{103}$, so findet man, ausgehend von den Näherungswerten $\frac{0}{1}, \frac{1}{0}$, durch fortgesetzte Mediation folgende Paare von Näherungswerten:

$$\frac{0}{1}, \frac{1}{0};\ \frac{1}{1}, \frac{1}{0};\ \frac{2}{1}, \frac{1}{0};\ \frac{2}{1}, \frac{3}{1};\ \frac{2}{1}, \frac{5}{2};\ \frac{2}{1}, \frac{7}{3};\ \frac{9}{4}, \frac{7}{3};\ \frac{16}{7}, \frac{7}{3};$$
$$\frac{23}{10}, \frac{7}{3};\ \frac{23}{10}, \frac{30}{13};\ \frac{23}{10}, \frac{53}{23};\ \frac{23}{10}, \frac{76}{33};\ \frac{23}{10}, \frac{99}{43};\ \frac{23}{10}, \frac{122}{53};\ \frac{23}{10}, \frac{145}{63};\ \frac{23}{10}, \frac{168}{73};$$
$$\frac{23}{10}, \frac{191}{83};\ \frac{23}{10}, \frac{214}{93};\ \frac{23}{10}, \frac{237}{103}.$$

Aus ihnen geht die einfache Reihe der Näherungswerte:

$$(91)\quad \frac{1}{1}, \frac{2}{1}, \frac{3}{1}, \frac{5}{2}, \frac{7}{3}, \frac{9}{4}, \frac{16}{7}, \frac{23}{10}, \frac{30}{13}, \frac{53}{23}, \frac{76}{33}, \frac{99}{43}, \frac{122}{53}, \frac{145}{63},$$
$$\frac{168}{73}, \frac{191}{83}, \frac{214}{93}, \frac{237}{103}$$

hervor, deren Anzahl gleich 18 ist. — Nimmt man nun zunächst $k = 3$ also $\varepsilon_1 = 1$, so ist die erste der Reihen (90) identisch mit der folgenden:

$$(91^a)\quad \frac{1}{1}, \frac{2}{1}, \frac{3}{1};$$

das nächste Paar von Näherungswerten ist $\frac{3}{1}, \frac{2}{1}$; da aber $\frac{m}{n}$ nicht mehr zwischen $\frac{3}{1}, \frac{5}{2}$ liegt, so ist $q' = 1$; wählt man nun $k_1 = 2$ also $\varepsilon_2 = 1$, so geht als zweite der Reihen (90) die folgende:

$$(91^b)\quad \frac{2}{1}, \frac{5}{2}$$

hervor. Das nächste Paar Näherungswerte sind die beiden Zahlen $\frac{5}{2}, \frac{2}{1}$; da aber $\frac{m}{n}$ nicht mehr zwischen $\frac{5}{2}, \frac{7}{3}$ liegt, so ist $q'' = 1$; für $k_2 = 1$ also $\varepsilon_3 = -1$ findet sich als dritte der Reihen (90) das einzige Glied

$$(91^c)\quad \frac{2}{1}.$$

Das nächste Paar Näherungsbrüche ist $\frac{2}{1}, \frac{7}{3}$; da jedoch $\frac{m}{n}$ nicht mehr zwischen $\frac{2}{1}, \frac{9}{4}$ liegt, findet sich $q''' = 1$, und bei der Wahl $k_3 = 1$ also $\varepsilon_4 = -1$ kommt als neue Reihe (90) die einzelne Zahl

$$(91^d)\quad \frac{7}{3}.$$

Nun ist das nächste Paar von Näherungswerten $\frac{7}{3}, \frac{9}{4}$, und man

findet, dafs $\frac{m}{n}$ zwischen $\frac{7}{3}$ und jeder der Zahlen $\frac{16}{7}, \frac{23}{10}$ aber nicht mehr zwischen $\frac{7}{3}$ und $\frac{30}{13}$ liegt; mithin ist $q^{(4)} = 3$; wählt man $k_4 = 4$ also $\varepsilon_5 = 1$, so ergiebt sich als nächste der Reihen (90) die folgende:

$$(91^e) \qquad \frac{9}{4}, \frac{16}{7}, \frac{23}{10}, \frac{30}{13}$$

und als nächstes Paar von Näherungswerten das Paar $\frac{30}{13}, \frac{23}{10}$; nun ist aber $\frac{m}{n}$ nicht mehr zwischen $\frac{30}{13}, \frac{53}{23}$ enthalten, mithin ist $q^{(5)} = 1$; bei der Wahl $k_5 = 1$ also $\varepsilon_6 = -1$ kommt als neue Reihe (90) das einzelne Glied

$$(91^f) \qquad \frac{23}{10}$$

und als nächstes Paar von Näherungswerten $\frac{23}{10}, \frac{30}{13}$; da man nunmehr $\frac{m}{n}$ zwischen $\frac{23}{10}$ und jeder der auf $\frac{30}{13}$ in der Reihe (91) folgenden Zahlen enthalten findet, so wird $q^{(6)} = 9$ und man kann $k_6 = 9$ wählen, womit die letzte der Reihen (90) die nachstehende:

$$(91^g) \qquad \frac{53}{23}, \frac{76}{33}, \frac{99}{43}, \frac{122}{53}, \frac{145}{63}, \frac{168}{73}, \frac{191}{83}, \frac{214}{93}, \frac{237}{103}$$

und die Rechnung beendet wird.

Die sieben mit (91^a) bis (91^g) bezeichneten Wertreihen bilden also in diesem Falle das System (90) aller Näherungswerte (91), doch findet sich, entsprechend den Werten $\varepsilon_1 = 1$, $\varepsilon_2 = 1$, $\varepsilon_5 = 1$, das vorletzte Glied der zugehörigen Reihe gleich dem ersten der folgenden Reihe. Während hiernach für $\frac{m}{n}$ der Kettenbruch

$$\frac{237}{103} = 3 - \cfrac{1}{2 - \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 - \cfrac{1}{1 + \cfrac{1}{9}}}}}}$$

gewonnen wird, ist die Summe seiner Teilnenner

$$3 + 2 + 1 + 1 + 4 + 1 + 9 = 21$$

d. h. um die Anzahl 3 der positiven ε_i gröfser als die Anzahl 18 der Näherungswerte (91), genau wie es der zuvor hergeleitete Satz verlangt.

16. Derselbe Satz giebt die Handhabe, eine bereits in Nr. 8 gestellte Frage zu beantworten, nämlich a n z u g e b e n, w e l c h e u n t e r d e n K e t t e n b r u c h e n t w i c k l u n g e n, d i e f ü r e i n e n B r u c h $w = \frac{m}{n}$ m ö g l i c h s i n d, d i e l ä n g s t e s e i. Es ist diejenige Entwicklung,

bei welcher die einzelnen Divisionen sämtlich nach dem gröfsten Reste ausgeführt werden. Wird nämlich an einer bestimmten Stelle des Algorithmus die Division in solcher Weise angestellt, dafs der Rest $\frac{\pm 1}{w'}$ absolut gröfser als $\frac{1}{2}$, sein Nenner w' also kleiner als 2 ist, so nimmt der Kettenbruch für $\frac{m}{n}$ an der entsprechenden Stelle eine der beiden Gestalten

$$k_i - \cfrac{\varepsilon_{i+1}}{1 + \cfrac{1}{k_{i+2} - \cfrac{\varepsilon_{i+3}}{k_{i+3} - \cdots}}} \tag{92}$$

oder

$$k_i - \cfrac{\varepsilon_{i+1}}{2 - \cfrac{1}{k_{i+2} - \cfrac{\varepsilon_{i+3}}{k_{i+3} - \cdots}}} \tag{93}$$

an, sodafs in dem Kettenbruche k, welcher der Voraussetzung entspricht, nur Teilnenner $1 +$ oder $2 -$ auftreten können. Lautet nun der Anfang des Kettenbruches

$$q + \quad \text{oder} \quad (q+1) -,$$

so entspricht diesem Anfange nach den Ausführungen der vorigen Nr. stets eine Anzahl q von Näherungswerten für $\frac{m}{n}$, jedem Teilnenner $1 +$, gleichfalls jedem Teilnenner $2 -$ gehört ein einziger Näherungswert zu, und somit ist, wenn γ die Anzahl der Teilnenner des Kettenbruchs k bezeichnet, $q + \gamma$ die Anzahl der Näherungswerte von $w = \frac{m}{n}$. Sei jetzt k' irgend ein anderer der Kettenbrüche für diese Gröfse. Beachtet man, dafs ein Teilnenner $1 -$ nicht vorkommen kann, denn einem solchen würde im modifizierten Euclidischen Algorithmus eine Gleichung

$$n_{i-2} = 1 \cdot n_{i-1} - n_i$$

entsprechen, aus welcher $n_{i-2} < n_{i-1}$ hervorginge, während das Gegenteil der Fall ist; bemerkt man weiter, dafs jedem Teilnenner $1 +$ sowie $2 -$ je ein Näherungswert, jedem Teilnenner $2 +$ oder $k_i \pm$ (für $k_i > 2$) mehr als ein Näherungswert entspricht, so findet man, wenn γ' die Anzahl der Teilnenner von k' bezeichnet, die Anzahl der Näherungswerte $\overline{\gtrless}\, q + \gamma'$, jenachdem in k' nur Teilnenner $1 +$ und $2 -$ vorkommen oder nicht; im letzteren Falle wäre daher $\gamma' < \gamma$ d. h. der Kettenbruch k' kürzer als k; im ersteren Falle wäre $\gamma' = \gamma$, beide Kettenbrüche also gleich lang. Dann sind sie aber auch, wie leicht zu sehen, identisch. Denn hat k die Gestalt $q + \frac{1}{w'}$, wo mit-

hin $\frac{1}{w'} > \frac{1}{2}$, $w' < 2$ ist, so mufs auch k' die Gestalt $q + \frac{1}{w''}$ haben und demnach $w'' = w'$ sein; sonst hätte nämlich k' die Gestalt $q + 1 - \frac{1}{w''}$, wo nun $\frac{1}{w''} = 1 - \frac{1}{w'} < \frac{1}{2}$ also $w'' > 2$ wäre, und die weitere Entwicklung von k' könnte nicht blos Teilnenner $1+$ und $2-$ haben. Desgleichen hat, wenn k die Gestalt $q + 1 - \frac{1}{w'}$ hat, wobei $w' < 2$ ist, auch k' die Gestalt $q + 1 - \frac{1}{w''}$, sodafs nun $w'' = w'$ wäre, denn andernfalls wäre $k' = q + \frac{1}{w''}$, wo $\frac{1}{w''} = 1 - \frac{1}{w'} < \frac{1}{2}$ also $w'' > 2$ wäre, und die weitere Entwicklung von k' könnte wieder nicht ausschliefslich Teilnenner $1+$, $2-$ aufweisen. Somit ist entweder

$$k = q + \frac{1}{w'} = k'$$

oder

$$k = q + 1 - \frac{1}{w'} = k';$$

aus der weiteren Entwicklung von w' im Kettenbruche k ergiebt sich aber auf dieselbe Weise auch die weitere Übereinstimmung der beiden Kettenbrüche k und k'. Nur der Schlufs derselben könnte verschieden sein: denn, endet k mit $1 + \frac{1}{2}$, so darf man dafür auch $2 - \frac{1}{2}$ setzen, und umgekehrt; der Kettenbruch k hat mithin zwei Formen von gleicher Ausdehnung, mit einer derselben aber wäre der Kettenbruch k' identisch, wenn anders er nicht kürzer ist als k.

Wir fügen diesem Satze den weiteren hinzu: Unter allen Kettenbrüchen oder **Euclid**ischen Algorithmen für $\frac{m}{n}$ ist keiner kürzer als derjenige, bei welchem sämtliche Divisionen nach dem kleinsten Reste ausgeführt werden. In der That, wird an einer Stelle des Algorithmus im Gegenteil die Division nach dem gröfsten Reste ausgeführt, so hat der Kettenbruch an dieser Stelle eine der beiden Formen (92) oder (93), die man ohne Mühe in die folgenden überführen kann:

$$(92^a) \qquad (k_i - \varepsilon_{i+1}) + \cfrac{\varepsilon_{i+1}}{(k_{i+2} + 1) - \cfrac{\varepsilon_{i+3}}{k_{i+3}} \cdots},$$

$$(93^a) \qquad (k_i - \varepsilon_{i+1}) + \cfrac{\varepsilon_{i+1}}{2 + \cfrac{1}{(k_{i+2} - 1) - \cfrac{\varepsilon_{i+3}}{k_{i+3}} \cdots}},$$

bei deren erster die Anzahl der Teilnenner kleiner, bei deren zweiter sie ebenso grofs ist, wie vorher. Da, wie schon bemerkt, ein Teilnenner 1 — nicht vorkommen kann, so ist die Kombination $k_{i+2} = 1$, $\varepsilon_{i+3} = 1$ in (92) ausgeschlossen, folglich hat das letzte Glied in (92[a]) nicht die Gestalt 2 —; nimmt man daher an, die betrachtete Stelle (92) des Kettenbruchs sei die letzte derjenigen, wo die Division nach dem gröfsten Reste ausgeführt wird, so wird diese Stelle durch die Umformung (92[a]) eliminiert und dabei die Anzahl der Teilnenner verringert. Desgleichen geschieht die Elimination, falls die letzte Stelle der angegebenen Art die Form (93) hat, durch die Umformung (93[a]) sobald $k_{i+2} > 3$ ist. Nun kann k_{i+2} nicht 1 sein, denn sonst müfste $\varepsilon_{i+3} = -1$ sein und es folgte in (93) auf den Teilnenner 2 — der Teilnenner 1 +, gegen die Voraussetzung; wäre aber $k_{i+2} = 2$, so müfste dieser Voraussetzung entsprechend $\varepsilon_{i+3} = -1$ sein und in (93[a]) träte dann der Teil

$$2 + \frac{1}{1 +} \frac{1}{k_{i+3} - \cdots}$$

ein, aus welchem aber durch die Umformung (92[a]) unter Verringerung der Anzahl der Glieder der Teilnenner 1 + fortgeschafft und somit jene letzte Stelle von der vorausgesetzten Art eliminirt werden könnte. Wäre endlich $k_{i+2} = 3$, $\varepsilon_{i+3} = 1$, so würde in (93[a]) der Teil

$$2 + \frac{1}{2 -} \frac{1}{k_{i+3} - \cdots} \tag{94}$$

eingeführt; dieser Teil würde

$$2 + \frac{1}{2 -} \frac{1}{k_{i+3}},$$

wenn k_{i+3} der letzte Teilnenner wäre, würde also für $k_{i+3} = 1$ mit $2 + \frac{1}{1} = 3$, für $k_{i+3} > 1$ nach der zweiten Umformung mit

$$3 - \frac{1}{2 +} \frac{1}{k_{i+3} - 1}$$

identisch, und der Teilnenner 2 — wäre verschwunden; ist aber k_{i+3} noch nicht der letzte Teilnenner, so kann man den Teil (94) mittels der Umformung (93[a]) behandeln, u. s. w. So wird man zuletzt durch eine begrenzte Reihe von Umformungen, bei denen die Anzahl der Teilnenner nicht zunehmen, sich höchstens nur verringern kann, den letzten Teilnenner 2 — aus dem Kettenbruche eliminiert haben.

Wird alsdann aber auf gleiche Weise successive jede der etwa noch vorhandenen früheren Stellen derselben Art behandelt, so führt man bei einer möglichen Verringerung der Anzahl der Teilnenner den gegebenen Kettenbruch in denjenigen über, bei welchem sämt-

liche Divisionen nach dem kleinsten Reste ausgeführt werden. Mithin kann dessen Gliederzahl nicht gröfser sein als die des ursprünglichen d. h. des beliebig gewählten Kettenbruchs für $\frac{m}{n}$.

Durch diesen von Vahlen (a. a. O.) abgeleiteten Satz erhält die Behauptung, welche schon Kronecker in seinen zahlentheoretischen Vorlesungen (s. Kronecker, *Vorlesungen über Mathematik*, 2. Teil, *Vorl. üb. allg. Arithmetik* I, herausg. von K. Hensel, 1901, p. 118) ausgesprochen hat, dafs der besagte Kettenbruch von allen der kürzeste sei, in genauerer Fassung ihre Bestätigung.

17. In Nr. 11 ist bereits bemerkt worden, dafs jeder (positive) rationale Bruch in einer gewissen Fareyschen Reihe auftreten mufs. Da die letzteren aber aus den Gliedern $\frac{0}{1}, \frac{1}{0}$ durch wiederholte Mediationen gewonnen werden, so findet man alle positiven rationalen Werte, wenn man, von den beiden Brüchen $\frac{0}{1}, \frac{1}{0}$ ausgehend, fort und fort andere durch Mediation bildet. Diese Operation besteht darin, aus zwei Brüchen $\frac{r}{u}, \frac{s}{v}$ den neuen Bruch $\frac{r+s}{u+v}$ zu bilden, und so wird man naturgemäfs zur Betrachtung der sämtlichen Zahlen geführt, welche aus zwei gegebenen Zahlen r, s durch successive Mediationen entstehen, d. i. dahin geführt, die folgenden Reihen von Zahlen aufzustellen:

$$r,\ r+s,\ s$$
$$r,\ 2r+s,\ r+s,\ r+2s,\ s$$
$$r,\ 3r+s,\ 2r+s,\ 3r+2s,\ r+s,\ 2r+3s,\ r+2s,\ r+3s,\ s$$
$$\dots\dots\dots\dots\dots\dots,$$

deren Gesamtheit wir mit Stern (*J. f. Math.* 55, 1858, p. 193; s. dazu auch Brocot, *calcul des rouages par approximation*, Paris 1862) die Entwicklung (r, s) nennen wollen, während deren eben angedeutete einzelnen Reihen durch $(r, s)_1, (r, s)_2, \dots$ allgemein die p^{te} derselben durch $(r, s)_p$ bezeichnet werden sollen.

Allgemein wird jede dieser Reihen, wie die drei zuvor aufgeschriebenen, durch das Mittelglied $r+s$ in zwei Hälften geteilt, deren sämtliche Glieder, unter k, l positive ganze Zahlen verstanden, die Form $kr+ls$ haben und symmetrisch zum Mittelgliede gebildet auftreten müssen, insofern zwei gleich weit von den Enden einer Reihe abstehende Glieder die Gestalt

$$kr+ls, \quad lr+ks$$

darbieten werden. Die Glieder einer Reihe finden sich auch in jeder der folgenden wieder, und man kann alle Glieder einer Reihe unterscheiden in Stammglieder d. h. solche, die bereits in der vorhergehenden vorhanden waren, und Summenglieder d. h. solche, die

als Summe von zwei benachbarten Gliedern der vorhergehenden Reihe neu in der betrachteten auftreten. Zwei oder mehr aufeinanderfolgende Glieder einer Reihe sollen als eine in derselben enthaltene Gruppe von Gliedern bezeichnet werden.

Ist A_p die Anzahl der Glieder in der p^{ten} Reihe, so findet sich sogleich die Beziehung

$$A_p = 2A_{p-1} - 1$$

und daraus

(95) $$A_p = 2^p + 1.$$

Bezeichnet dagegen S_p die Summe der Glieder in der p^{ten} Reihe, so findet man für diese durch die Bemerkung, daſs jedes Glied der $(p-1)^{\text{ten}}$ Reihe sich auch in der p^{ten} vorfindet, auſserdem darin aber sowohl mit dem ihm voraufgehenden, als mit dem ihm folgenden zu einer Summenzahl sich verbindet, ausgenommen das Anfangs- und das Endglied, welche letzteres nur mit einer Zahl (der resp. ihm folgenden oder ihm voraufgehenden) thun, die Rekursionsformel:

$$S_p = 3S_{p-1} - r - s,$$

aus welcher ohne Mühe die Bestimmung

(96) $$S_p = \frac{3^p + 1}{2} \cdot (r + s)$$

hervorgeht.

Um die weiteren Eigenschaften der Entwicklung (r, s) zu ermitteln, genügt es im Grunde, die erste Hälfte jeder der Reihen $(r, s)_p$ zu betrachten. Da nun deren Glieder $kr + ls$ aus r und $r + s$ d. i. aus

$$1 \cdot r + 0 \cdot s \quad \text{und} \quad 1 \cdot r + 1 \cdot s$$

durch wiederholte Mediation entstehen, so werden die Zahlenkoeffizienten k, l auf genau gleiche Weise aus den Zahlen 1, 1 resp. 0, 1 entstehen oder die entsprechenden Glieder der beiden Reihen $(1, 1)_p$ und $(0, 1)_p$ sein. Betrachtet man aber die Entwicklung $(0, 1)$:

$$0,\ 1,\ 1$$

$$0,\ 1,\ 1,\ 2,\ 1$$

$$0,\ 1,\ 1,\ 2,\ 1,\ 3,\ 2,\ 3,\ 1$$

u. s. w., so erkennt man sofort, daſs die Reihe $(0, 1)_{p-1}$ die erste, die Reihe $(1, 1)_{p-1}$ die zweite Hälfte von $(0, 1)_p$, oder daſs $(0, 1)_p$ aus den beiden aneinander geschlossenen Reihen $(0, 1)_{p-1}$ und $(1, 1)_{p-1}$ zusammengesetzt ist. Hierdurch wird man zur Bildung der Reihe $(0, 1)_p$ oder der Entwicklung $(0, 1)$ auf die Glieder 0, 1 und die Reihen $(1, 1)_1, (1, 1)_2, \ldots (1, 1)_{p-1}$ d. h. auf die Entwicklung $(1, 1)$ zurückgeführt. Um demnach die Eigenschaften der Entwicklung (r, s) zu ermitteln, wird es darauf ankommen, zuvörderst diejenigen der speziellen Entwicklung $(1, 1)$ festzustellen.

18. Hier steht offenbar am Anfang und am Ende jeder Reihe, aber auch nur dort, die Einheit; das Mittelglied ist 2; symmetrische Glieder sind einander gleich. Ist ferner a, b, c eine Gruppe von drei aufeinanderfolgenden Gliedern der Reihe $(1, 1)_p$, so wird entweder b ein Summenglied also

$$a + c = b \tag{97}$$

sein, oder aber b ist bereits in einer der voraufgehenden Reihen, etwa in der $(p-i)^{\text{ten}}$ Reihe als Summenglied entstanden; heifsen also a', c' die darin b umgebenden Glieder, so hat man in der Reihe $(1, 1)_{p-i}$ die Gruppe a', b, c', für welche

$$a' + c' = b$$

ist, und aus welcher in der p^{ten} Reihe offenbar die Gruppe

$$a = a' + ib, \quad b, \quad c = ib + c'$$

hervorgeht, sodafs

$$a + c = (2i + 1)b \tag{98}$$

gefunden wird, eine Formel, welche den vorigen Fall (97) als speziellen Fall mit umfafst. Hieraus ist sofort zu schliefsen, dafs zwei aufeinanderfolgende Glieder einer Reihe relativ prim sind; denn jeder gemeinsame Teiler von b, c würde zufolge (98) auch ein Teiler des nächst vorhergehenden Gliedes a, also ein gemeinsamer Teiler von a, b sein, u. s. w.; wäre schliefslich also auch ein Teiler des Anfangsgliedes der Reihe, d. i. der Einheit.

Jede positive ganze Zahl n tritt in der Entwicklung $(1, 1)$ auf; denn die erste Reihe beginnt mit 1, 2, also die folgende mit 1, 3, 2, die dritte mit 1, 4, 3, u. s. w., also die $(n-1)^{\text{te}}$ mit $1, n, n-1$; hier spätestens also wird die Zahl n als Summenglied eingeführt.

Aber auch jede Gruppe a, b zweier positiver teilerfremder Zahlen findet sich in der Entwicklung $(1, 1)$ vor. Zum Beweise darf man $a > b$ voraussetzen, denn die Gruppe a, b kommt immer gleichzeitig mit der Gruppe b, a in einer Reihe vor oder gleichzeitig nicht vor. Für zwei solche Zahlen besteht aber der Euclidische Algorithmus

$$a = qb + b_1$$
$$b = q_1 b_1 + b_2$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$b_{h-1} = q_h b_h + 1\,.$$

Nun findet sich in der $(b_h - 1)^{\text{ten}}$ Reihe am Anfange die Gruppe $1, b_h$, aus welcher in der $(q_h + b_h - 1)^{\text{ten}}$ Reihe die Gruppe

$$1 + q_h b_h = b_{h-1}, \; b_h$$

hervorgeht; aus dieser entsteht in der $(q_{h-1} + q_h + b_h - 1)^{\text{ten}}$ Reihe die Gruppe

$$b_{h-1},\ q_{h-1} b_{h-1} + b_h = b_{h-2}$$

u. s. f.; endlich in der

$$(q + q_1 + \cdots + q_{h-1} + q_h + b_h - 1)^{\text{ten}}$$

Reihe die behauptete Gruppe a, b. Aus dem Beweise ergiebt sich auch, wie die Nummer der Reihe ermittelt werden kann, in welcher diese Gruppe a, b sich findet. Man hat nur nötig, den gewöhnlichen Kettenbruch für $\frac{a}{b}$ aufzustellen:

$$\frac{a}{b} = q + \cfrac{1}{q_1 + \cdots + \cfrac{1}{q_h + \cfrac{1}{b_h}}};$$

ist die Summe der Teilnenner (einschliefslich des Anfangsgliedes) für diesen Kettenbruch gleich $p + 1$, so findet sich die Gruppe a, b in der Reihe $(1, 1)_p$; man darf auch sagen: die Glieder dieser Reihe haben die Eigenschaft, dafs der Quotient je zweier aufeinanderfolgender Glieder einen Kettenbruch liefert, für welchen die Summe der Teilnenner (einschliefslich des Anfangsgliedes) gleich $p + 1$ ist. Letztere Aussage folgt, wenn man das Voraufgehende mit dem ferneren Satze verbindet:

Jede Gruppe a, b tritt auch nur einmal in der Entwicklung $(1, 1)$ auf. Zunächst zeigen wir, dafs sie nicht in zwei verschiedenen Reihen angetroffen wird. Setzt man wieder, was zulässig ist, $a > b$ voraus, so mufs a in jeder Reihe, in welcher die Gruppe sich findet, offenbar Summenglied sein; deshalb befindet sich in dieser Reihe eine Gruppe β, a, b, wo $\beta < a$, also in der vorhergehenden Reihe die Gruppe β, b. Ist noch $\beta > b$ also wieder ein Summenglied, so käme in der jetzt nächstvorhergehenden Reihe eine Gruppe β', b vor, in welcher $\beta' < \beta$ ist, u. s. w. fort, bis man zu einer Reihe gelangen wird, in welcher eine Gruppe b', b sich vorfindet, wo $b' < b$ ist. In dieser voraufgehenden Reihe fände sich also eine Gruppe vor, bei welcher das bisher kleinere Glied der Gruppe a, b jetzt vielmehr zum gröfseren Gliede geworden ist. So fortfahrend kommt man notwendig in einer der vorhergehenden Reihen zu einer Gruppe $1, c$ oder $c, 1$. Da aber die Zahlen $\beta, \beta', b', \ldots$ eindeutig aus a, b hervorgehen, so ist die Anzahl i der Reihen, um welche man zurückgehen mufs, bis die Gruppe $1, c$ oder $c, 1$ erscheint, nur von a, b abhängig. Käme also a, b sowohl in $(1, 1)_p$ als auch in $(1, 1)_q$ vor, wo p, q verschieden gedacht sind, so fände sich die Gruppe $1, c$ resp. $c, 1$ sowohl in der $(p - i)^{\text{ten}}$ als $(q - i)^{\text{ten}}$ Reihe vor, wäh-

rend sie nur als Anfang resp. als Ende der $(c-1)^{\text{ten}}$ Reihe zu finden ist.

Aber auch in derselben Reihe $(1, 1)_p$ kann a, b nur einmal auftreten, denn sonst müfste die Gruppe $1, c$ oder $c, 1$ in der $(p-i)^{\text{ten}}$ Reihe offenbar auch mehrfach zu finden sein, was nicht der Fall ist.

Somit kommt in der That eine Gruppe a, b überhaupt nur einmal in der Entwicklung $(1, 1)$ vor.

19. Wenden wir uns nun wieder zum allgemeinen Falle, dem der Entwicklung (r, s) zurück, so dürfen wir uns auf die Voraussetzung beschränken, dafs r, s relativ prim sind, denn sonst hätten alle Glieder dieser Entwicklung, da sie die Form $kr + ls$ haben, den gemeinsamen Teiler von r, s ebenfalls, den wir offenbar ohne Einflufs auf die Gesetze der Entwicklung überall unterdrücken dürfen. Da ferner r, s in einer gewissen, etwa in der p^{ten} Reihe als eine Gruppe in der Entwicklung $(1, 1)$ auftreten, so wird die gesamte Entwicklung (r, s) nur einen mittleren Teil der folgenden Reihen dieser speziellen Entwicklung ausmachen und es werden daher die Gesetze der letzteren auch für jene Entwicklung Bestand behalten. Beachtet man ferner, dafs das allgemeine Glied der Entwicklungsreihe $(r', s')_p$ genau so aus r', s' gebildet ist, wie das entsprechende Glied der Reihe $(r, s)_p$ aus r und s, so erkennt man sofort, dafs jedes Glied der Reihe $(r \pm r', s \pm s')_p$ die Summe bezw. die Differenz der entsprechenden Glieder jener zwei Reihen ist, was ausgedrückt werden soll durch die symboliche Gleichung

$$(r, s)_p \pm (r', s')_p = (r \pm r', s \pm s')_p.$$

Aus dieser findet sich z. B.

$$(1, 2)_p - (1, 1)_p = (0, 1)_p.$$

Nun ist $(1, 2)_p$ offenbar die erste Hälfte der Reihe $(1, 1)_{p+1}$. Bezeichnet man daher mit a, α, α' gleichstellige d. h. etwa die h^{ten} Glieder der Reihen $(0, 1)_p$, $(1, 1)_p$, $(1, 1)_{p+1}$, so ergiebt sich aus der vorstehenden Gleichung die andere:

$$a = \alpha' - \alpha,$$

wobei zugleich offenbar $\alpha > a$ ist. Seien jetzt b resp. β, β' die auf a, α, α' folgenden Glieder jener Reihen; dann wird behauptet, dafs allgemein

$$\alpha\beta' - \alpha'\beta = 1 \tag{99}$$

sei. In der That bestätigt man dies für die ersten Reihen der Entwicklung $(1, 1)$ unmittelbar. Angenommen nun, es gelte auch für die p^{te} Reihe. Da aus α, β in der $p + 1^{\text{ten}}$ Reihe die Gruppe

$$\alpha, \ \sigma = \alpha + \beta, \ \beta,$$

aus α', β' in der $p+2^{\text{ten}}$ Reihe die Gruppe

$$\alpha',\ \sigma' = \alpha' + \beta',\ \beta'$$

hervorgeht, wobei offenbar α, α' in diesen genannten Reihen gleichstellige Glieder bleiben, so findet sich

$$\alpha\sigma' - \alpha'\sigma = \sigma\beta' - \sigma'\beta = \alpha\beta' - \alpha'\beta$$

und folglich wegen der für die p^{te} Reihe vorausgesetzten Gleichung (99) gleich 1; die Behauptung gilt deshalb auch für die $(p+1)^{\text{te}}$ Reihe und somit allgemein.

Daraus findet sich dann aber auch, da

$$a = \alpha' - \alpha, \quad b = \beta' - \beta$$

ist,

$$\alpha b - a\beta = 1; \tag{100}$$

zugleich sind a, b die kleinsten positiven ganzen Zahlen, welche dieser Gleichung genügen, denn jede andere Lösung der Gleichung

$$\alpha y - \beta x = 1$$

wäre $x = a - \alpha z$, $y = b - \beta z$ und gäbe, da $\alpha > a$, je nach dem ganzzahligen Werte, den man z erteilt, für x einen negativen Wert oder einen positiven Wert gröfser als a.

Nunmehr soll gezeigt werden, dafs jede Zahl $kr + ls$, wenn k, l positive, relativ prime Zahlen sind, in der Entwicklung (r, s) vorhanden ist. In der That wissen wir bereits, dafs die Gruppe k, l in einer bestimmten Reihe $(1, 1)_p$ sich findet; verstehen wir unter den zuvor mit α, β bezeichneten Zahlen diese Zahlen $\alpha = k$, $\beta = l$, so sind die mit a, b bezeichneten Zahlen die kleinsten positiven ganzen Zahlen x, y, welche der Gleichung

$$ky - lx = 1$$

genügen. Es wird nun hinreichen, die Behauptung unter der Annahme $k > l$ zu erhärten, da die Glieder $kr + ls$ und $lr + ks$ in der Entwicklung entweder beide oder keins von beiden vorkommen. Bei dieser Annahme erkennt man dann einfach, dafs l, b auch die kleinsten positiven ganzen Zahlen x, y sind, welche der Gleichung

$$ky - ax = 1$$

Genüge leisten. Zugleich erkennt man k, a als relative Primzahlen und schliefst daher, dafs k, a in einer gewissen Reihe $(1, 1)_q$ eine Gruppe bilden, sowie dafs l, b zwei mit ihnen gleichstellige Glieder der Reihe $(0, 1)_q$ und deshalb $kr + ls$ das k entsprechende Glied der Entwicklungsreihe $(r, s)_q$ darstellt.

Man kann noch hinzufügen, dafs eine Zahl $kr + ls$, bei welcher k, l **nicht** relativ prim sind, in der Entwicklung (r, s) **nicht** vorkommt. Denn nach Ende von Nr. 17 müssen k, l gleich-

stellige Glieder gewisser Reihen $(1, 1)_p$, $(0, 1)_p$ und daher wegen (100) ohne gemeinsamen Teiler sein.

Ist so nachgewiesen, dafs, falls k, l relativ prim sind, die Zahl $kr + ls$ in der Entwicklung vorhanden ist, so kann noch weiter ausgesagt werden, dafs sie auch nur einmal in dieser Entwicklung als Summenglied entsteht. Hierzu bemerke man zunächst Folgendes:

Sei $kr + ls$, $k'r + l's$ eine Gruppe in der Entwicklungsreihe $(r, s)_p$. Nach dem, was bereits über die Bildung der Zahlenkoeffizienten k, l aus den Elementen $1, 1$ resp. $0, 1$ gesagt worden, vertreten k, k' bezw. l, l' genau die Stelle der kurz zuvor mit α, β bezw. mit a, b bezeichneten Zahlen; demnach besteht die Beziehung

$$(101) \qquad kl' - k'l = 1$$

und l, l' sind die kleinsten positiven ganzen Zahlen, welche dieser Gleichung genügen.

Nimmt man nun an, die Zahl $kr + ls$ entstehe zwiefach als Summenglied, sodafs man zwei Gruppen hätte:

$$k_1 r + l_1 s, \quad kr + ls, \quad k'r + l's, \quad k > k'$$
$$k_2 r + l_2 s, \quad kr + ls, \quad k''r + l''s, \quad k > k'',$$

dann müfste nach (101) sowohl k', l' als k'', l'' die kleinste positive ganzzahlige Lösung der Gleichung

$$ky - lx = 1$$

darstellen also miteinander identisch sein, womit dann auch die vorigen zwei Gruppen einander gleich würden; dann wäre aber die Gruppe der beiden Zahlen $kr + ls$, $k'r + l's$ zwiefach in der Entwicklung (r, s), also auch in der Entwicklung $(1, 1)$ vorhanden, gegen das, was in voriger Nr. über die letztere ermittelt worden ist.

20. Ist jetzt n eine beliebig gegebene positive ganze Zahl, so kann dieselbe in der Entwicklung (r, s) nur auftreten, wenn sie in die Form

$$n = kr + ls$$

gesetzt werden kann, welche allen Gliedern dieser Entwicklung eigen ist, wobei k, l der Gleichung (101) zufolge relativ prim sein müssen. So oft sie aber in diese Form gesetzt werden kann, tritt sie dem soeben Bewiesenen gemäfs in der Entwicklung — zum ersten Male als Summenglied — auf. Dies führt zu der Aufgabe, festzustellen, wie oft die Gleichung

$$(102) \qquad n = kr + ls$$

in positiven ganzen, relativ primen Zahlen k, l auflösbar ist. Ihre sämtlichen ganzzahligen Auflösungen findet man, wenn man mit x_0, y_0 die kleinste positive Auflösung der Gleichung

(103) $$-ry + sx = 1$$

bezeichnet, sodaſs

(104) $$-ry_0 + sx_0 = 1$$

ist, nach Kap. 3 Nr. 5 durch die Formeln

(105) $$k = -y_0 n + sz, \quad l = x_0 n - rz,$$

in welchen z jede ganze Zahl bedeutet und aus denen

(106) $$kx_0 + ly_0 = z$$

hervorgeht. Sollen aber k, l positiv sein, so darf z nur eine der ganzen Zahlen sein, die zwischen $\frac{y_0 n}{s}$ und $\frac{x_0 n}{r}$ enthalten sind; sollen sie endlich relativ prim werden, so zeigen die Formeln (105), daſs notwendig z relativ prim gegen n gewählt werden muſs; geschieht dies aber, so werden auch k, l ohne gemeinsamen Teiler sein, da ein solcher wegen (106) stets auch in z, daher wegen (105) gleichzeitig in $x_0 n$, $y_0 n$ und, da x_0, y_0 wegen (104) relativ prim sind, auch in n enthalten sein müſste. Hiernach hat die Gleichung (102) soviel Auflösungen in relativ primen positiven ganzen Zahlen k, l, als es zwischen $\frac{y_0 n}{s}$, $\frac{x_0 n}{r}$ relativ prime Zahlen zu n giebt, und ebenso oft tritt n in der Entwicklung (r, s) als Summenglied auf.

Z. B. ist für $r = 1$, $s > 1$ die kleinste positive Auflösung der Gleichung (103)

$$x_0 = 1, \quad y_0 = s - 1.$$

Demnach tritt n in der Entwicklung $(1, s)$ oder $(s, 1)$ so oft als Summenglied auf, als es zwischen $\frac{s-1}{s} n$ und n, oder auch, als es zwischen 0 und $\frac{n}{s}$ relative Primzahlen zu n giebt.

Desgleichen findet sich für $r = 1$, $s = 1$ als kleinste positive Auflösung der Gleichung (103)

$$x_0 = 2, \quad y_0 = 1;$$

somit tritt n in der Entwicklung $(1, 1)$ so oft als Summenglied auf, als es zwischen n und $2n$, oder auch, als es zwischen 0 und n relative Primzahlen zu n giebt, also $\varphi(n)$-mal.

21. Noch kann man fragen, in welcher Entwicklungsreihe $(r, s)_p$ die Zahl $kr + ls$ sich als Summenglied findet. Um dies zu beantworten, nehmen wir zuerst $k > l$ an. Nennt man nun die Glieder, welche die Zahl $kr + ls$ umgeben, $k'r + l's$, $k''r + l''s$, sodaſs

$$kr + ls = (k'r + l's) + (k''r + l''s)$$

ist, so sind (nach Nr. 19) l', l; l, l'' resp. die kleinste positive ganzzahlige Auflösung der Gleichungen:

(107) $$k'y - kx = 1, \quad ky - k''x = 1,$$
sodaſs
(108) $$k'l - kl' = 1, \quad kl'' - k''l = 1$$
ist. Man denke nun $\frac{k}{l}$ in seinen gewöhnlichen Kettenbruch entwickelt:
(109) $$\frac{k}{l} = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots + \cfrac{1}{q_h}}}$$
und nenne seinen vorletzten Näherungsbruch $\frac{k_0}{l_0}$; indem man erforderlichenfalls den Schluſsnenner $q_h > 2$ durch $(q_h - 1) + \frac{1}{1}$ ersetzt, wodurch die Summe aller Teilnenner (einschlieſslich des Anfangsgliedes) nicht geändert wird, kann man bewirken, daſs
$$kl_0 - k_0 l = 1$$
wird, woraus, da $k_0 < k$, sich $k'' = k_0$, $l'' = l_0$ und, da $k = k' + k''$, $l = l' + l''$ ist, sich $k' = k - k_0$, $l' = l - l_0$ finden. Somit sind k', k'' ebenso wie k, k_0 relativ prim, und für
$$\frac{k'}{k''} = \frac{k - k_0}{k_0}$$
ergiebt sich mit Rücksicht auf Nr. 6 der folgende Kettenbruch:
$$\frac{k'}{k''} = q_h - 1 + \cfrac{1}{q_{h-1} + \cdots + \cfrac{1}{q}},$$
für welchen die Summe aller Teilnenner einschlieſslich des Anfangsgliedes gleich p ist, wenn man die Summe all' dieser Nenner für den Kettenbruch (109):
$$q + q_1 + q_2 + \cdots + q_h = p + 1$$
setzt. Nach den Sätzen der Nr. 18 kommt mithin die Gruppe k', k'' in der Entwicklung $(1, 1)$ und demnach auch die Gruppe $k'r + l's$, $k''r + l''s$ in der Entwicklung (r, s) in der $(p-1)^{\text{ten}}$, folglich das Summenglied $kr + ls$ in der p^{ten} Reihe der letztgenannten Entwicklung vor. Man erhält also den Satz:

Hat die Summe der Teilnenner einschlieſslich des Anfangsgliedes im Kettenbruch für $\frac{k}{l}$ den Wert $p + 1$, so findet sich $kr + ls$ in der Reihe $(r, s)_p$ als Summenglied vor.

Beim Beweise dieses Satzes war zwar $k > l$ vorausgesetzt worden; indessen, falls das Gegenteil der Fall wäre, brauchte man statt des Kettenbruchs für $\frac{k}{l}$ nur denjenigen für $\frac{l}{k}$ zu betrachten, was im Ausspruche des Satzes nichts ändert, da für den letzteren Bruch die

Summe der Teilnenner (einschliefslich des Anfangsgliedes) die gleiche ist, wie für den erstern.

22. Wir beschliefsen diesen Abschnitt mit einer Anwendung der eben geführten Untersuchung auf die Wertbestimmung einer numerischen Funktion, auf welche **Eisenstein** gelegentlich seiner Ableitung der höheren Reziprozitätsgesetze geführt worden ist.*)

Die Eisensteinsche Funktion ist durch folgende Bestimmungen definiert:

Für positive ganze, relativ prime Werte ϱ, σ soll

$$f(\varrho, \sigma) = f(\varrho, \varrho + \sigma) + f(\varrho + \sigma, \sigma)$$

sein, so oft $\varrho + \sigma$ kleiner ist als eine gegebene ungerade Primzahl n; dagegen

$$f(\varrho, \sigma) = \sigma, \quad \text{wenn} \quad \varrho + \sigma = n,$$

$$f(\varrho, \sigma) = 0, \quad \text{wenn} \quad \varrho + \sigma > n$$

ist.

Wenn diese Funktion für gegebene Argumente r, s angegeben werden soll, deren Summe kleiner als n anzunehmen ist, denn sonst wäre $f(r, s)$ durch die Definition unmittelbar gegeben, so wird man auszugehen haben von der Gleichung

$$f(r, s) = f(r, r + s) + f(r + s, s);$$

diese verwandelt sich durch Substitution der Funktionswerte zur Rechten in die folgende:

$$f(r, s) = f(r, 2r + s) + f(2r + s, r + s) + f(r + s, r + 2s) + f(r + 2s, s)$$

u. s. w. Man sieht auf solche Weise die Glieder der successiven Entwicklungsreihen $(r, s)_p$ entstehen, ein jedes bis auf das erste und letzte zweimal. Wird bei diesen fortschreitenden Substitutionen in einer der Funktionen $f(\varrho, \sigma)$ die Summe der Argumente gleich n, so wird ihr Wert dem zweiten der Argumente σ gleich und bleibt fortan in der weiteren Umformung unverändert erhalten; sobald dagegen in einer Funktion $f(\varrho, \sigma)$ die Summe der Argumente den Wert n überschreitet, fällt diese Funktion ferner aus der Betrachtung heraus, da sie Null wird. Da nun die Argumente ϱ, σ zwei aufeinanderfolgende Glieder derselben Entwicklungsreihe $(r, s)_p$ sind, also von den Formen

$$\varrho = k'r + l's, \quad \sigma = k''r + l''s$$

*) S. darüber Eisenstein, *Journ. f. Math.* 39, 1850, p. 351; in den *Berl. Monatsb.* 1850 p. 36 gab dann Eisenstein seine Bestimmung der gedachten Funktion und eine Reihe von Sätzen über die Entwicklung (r, s), welche in der hier in den wesentlichsten Punkten reproduzierten Arbeit später Stern auf Eisensteins Anregung in elementarer Weise herleitete.

sein werden, so wird schliefslich die ganze rechte Seite gleich der Summe aller derjenigen Glieder $\sigma = k''r + l''s$ der Entwicklung (r, s), in Zeichen:

$$f(r, s) = \sum (k''r + l''s) \tag{110}$$

sein, für welche

$$\varrho + \sigma = (k'r + l's) + (k''r + l''s) = n$$

ist, d. h. für welche n einem Summengliede derselben Entwicklung gleich ist. Nun tritt n nach Nr. 20 so oft in dieser Entwicklung als Summenglied auf, als es relative Primzahlen z zwischen $\frac{y_0 n}{s}$ und $\frac{x_0 n}{r}$ giebt; ist nämlich z irgend eine dieser Zahlen und

$$k = -y_0 n + sz, \quad l = x_0 n - rz, \tag{111}$$

so ist $n = kr + ls$ und es giebt zwei aufeinanderfolgende Glieder $k'r + l's$, $k''r + l''s$ einer Entwicklungsreihe $(r, s)_p$ derart, dafs

$$kr + ls = (k'r + l's) + (k''r + l''s), \tag{112}$$

nämlich $k = k' + k''$, $l = l' + l''$ ist; zugleich besteht die Beziehung

$$k'l'' - k''l' = 1. \tag{113}$$

Multipliziert man (112) mit k'' und berücksichtigt (113), so entsteht die Kongruenz

$$(k' + k'')(k''r + l''s) \equiv s \pmod{n},$$

durch Multiplikation von (112) mit l'' diese andere:

$$(l' + l'')(k''r + l''s) \equiv -r \pmod{n};$$

wegen (111) ist ferner

$$k' + k'' \equiv sz, \quad l' + l'' \equiv -rz.$$

Da aber ein Primfaktor von n nur in einer der beiden relativ primen Zahlen r, s aufgehen kann, so erschliefst man aus den vorstehenden Kongruenzen die folgende neue:

$$z(k''r + l''s) \equiv +1 \pmod{n},$$

und auf analogem Wege die andere:

$$z(k'r + l's) \equiv -1 \pmod{n}.$$

Diese lassen sich auch dahin fassen, dafs man sagt: die Zahl z sei der socius des Gliedes $k''r + l''s$, $n - z$ aber der socius des Gliedes $k'r + l's$, aus denen beiden $n = kr + ls$ als Summenglied in der Entwicklung (r, s) entsteht.

Fafst man hiernach die Gleichung (110) — wie es für die Eisensteinsche, die Reziprozitätsgesetze betreffende Untersuchung genügend ist — als eine Kongruenz (mod. n) auf, so läfst sich die Formel aufstellen:

$$f(r, s) \equiv \sum \frac{1}{z} \pmod{n}, \tag{114}$$

worin die Summe über alle zu n primen Zahlen zwischen den Grenzen $\frac{y_0 n}{s}$, $\frac{x_0 n}{r}$ zu erstrecken ist, eine Formel, wie sie in der That a. a. O. von Eisenstein gegeben worden ist.

Z. B. hat man zufolge der vorletzten Bemerkung in Nr. 20, wenn man $r = 1$, $s = 2$ wählt, wo dann z jede zu n prime Zahl zwischen den Grenzen $\frac{n}{2}$ und n d. h., wenn n als Primzahl gedacht wird, jede der Zahlen

$$\frac{n+1}{2}, \frac{n+3}{2}, \cdots n-1$$

bedeutet, die Kongruenz

$$f(1, 2) \equiv \frac{1}{\frac{n+1}{2}} + \frac{1}{\frac{n+3}{2}} + \cdots + \frac{1}{n-1} \pmod{n}, \tag{115}$$

der man auch, wie an späterer Stelle (Kap. 5 Nr. 6) gezeigt werden wird, diese andere Form:

$$f(1, 2) \equiv \frac{2^n - 2}{n} \pmod{n} \tag{116}$$

geben kann. —

Fünftes Kapitel.

Die Sätze von Fermat und von Wilson.

1. Nachdem wir in den letzten drei Kapiteln die Folgerungen aus der Grundformel

$$m = qn + r$$

nach verschiedenen Richtungen hin verfolgt haben, knüpfen wir jetzt insbesondere an den in Nr. 5 des dritten Kapitels erhaltenen Satz wieder an, nach welchem die Produkte aus einer zum Modulus n primen Zahl a in die Glieder eines reduzierten Restsystems wieder ein solches System (mod. n) ausmachen. Sind also

$$r_1, r_2, \ldots r_{\varphi(n)}$$

ein System dieser Art, so sind die Produkte

$$ar_1, ar_2, \ldots ar_{\varphi(n)}$$

in ihrer Gesamtheit denselben Zahlen und demnach auch das Produkt der letztern dem Produkte der ersteren kongruent:

$$a^{\varphi(n)} \cdot r_1 r_2 \cdots r_{\varphi(n)} \equiv r_1 r_2 \cdots r_{\varphi(n)} \pmod{n}.$$

Der gemeinsame Faktor beider Seiten aber ist prim gegen n und kann daher (s. Kap. 3 Nr. 2) unterdrückt werden. So gelangt man zur Kongruenz

(1) $$a^{\varphi(n)} \equiv 1 \pmod{n}$$

oder zu dem Satze: Die $\varphi(n)^{\text{te}}$ Potenz jeder zu n primen Zahl läfst, durch n geteilt, den Rest 1.

Ist insbesondere der Modulus n eine Primzahl p, so besteht für jede durch p nicht teilbare Zahl a die Kongruenz

(2) $$a^{p-1} \equiv 1 \pmod{p}$$

oder auch diese, ihr völlig gleichbedeutende:

(2ᵃ) $$a^p \equiv a \pmod{p},$$

welche indessen vor der ersteren den Vorzug hat, auch für solche Zahlen a zu gelten, die durch p teilbar sind, mithin für jede ganze Zahl a zu bestehen.

Der einfachere, auf einen Primzahlmodulus bezügliche Satz heifst der **Fermat**sche Satz, weil er bereits von Fermat (*op. math.*, Tolosae 1679; eine Gesamtausgabe seiner Werke unternahmen 1891 Paul Tannery und Ch. Henry) gegeben worden ist, freilich ohne Beweis, den jedoch Fermat geben zu können behauptet hat. Zuerst bewies ihn L. Euler (auch Leibnitz soll einen Beweis desselben besessen haben (s. Gaufs, *Disqu. Ar. art.* 50 Anmerkung)), und Euler ist dann auch zuerst zu dem allgemeinen Satze (1) geführt worden (*Petrop. Comm. nov.* 8, 1760/61, p. 74 = *Comment. Ar. coll.* 1, p. 274), den man den verallgemeinerten Fermatschen Satz nennt.

Jener erste, sehr einfache Eulersche Beweis (*Petrop. Comm.* 8, 1736, p. 141 = *Comm. Ar. coll.* 1, p. 21), der sich ähnlich auch bei Lambert (*Act. Erudit.* 1769, p. 109) findet, beruht auf dem binomischen Satze. Nach diesem Satze und zufolge Nr. 12 des 2. Kapitels ist

$$(a+1)^p \equiv a^p + 1 \pmod{p}$$

folglich

$$(a+1)^p - (a+1) \equiv a^p - a \pmod{p};$$

ist also $a^p \equiv a$, so ist auch $(a+1)^p \equiv a+1$, weil aber $1^p \equiv 1$ ist, folgt hiernach $2^p \equiv 2$, also auch $3^p \equiv 3$, u. s. w., allgemein also die Kongruenz (2ᵃ).

Statt des binomischen Satzes kann man sich auch des polynomischen bedienen (s. Gaufs, *Disqu. Ar. art.* 51), nach welchem

$$(\alpha+\beta+\gamma+\cdots)^p \equiv \alpha^p + \beta^p + \gamma^p + \cdots \pmod{p};$$

werden nämlich die Zahlen $\alpha, \beta, \gamma, \ldots$, deren Anzahl a sei, sämtlich der Einheit gleich vorausgesetzt, so ergiebt sich ohne weiteres die Kongruenz (2ᵃ). Euler gab (*Petr. Comm. nov.* 7, 1758/59, p. 49 = *Comm. Ar. coll.* 1, p. 260) noch einen andern Beweis des Fermatschen Satzes, der im wesentlichen mit dem von Gaufs (*Disqu. Ar. art.* 49) gegebenen übereinkommt; der letztere wird an späterer Stelle (Kap. 7 Nr. 1) in verallgemeinerter Fassung dargestellt werden.

2. Hier fügen wir dagegen noch einen, auf ganz anderer Grundlage beruhenden Beweis an, welchen man Lagrange (*Ac. de Berlin, Nouv. mém.* 2, 1773, année 1771, p. 125 = *Oeuv.* 3, p. 425) verdankt und der sogleich noch einen zweiten wichtigen Satz zu Tage fördern wird. Entwickelt man das Produkt

$$(x+1)(x+2)\cdots(x+p-1) \tag{3}$$

nach Potenzen von x, so entsteht ersichtlich ein Ausdruck von der Form

$$x^{p-1} + A_1 x^{p-2} + A_2 x^{p-3} + \cdots + A_{p-2}x + A_{p-1}, \tag{4}$$

dessen Koeffizienten ganze Zahlen sind, nämlich

$$\begin{aligned} A_1 &= 1 + 2 + 3 + \cdots + (p-1) \\ A_2 &= 1\cdot 2 + 1\cdot 3 + \cdots + 2\cdot 3 + \cdots + (p-2)(p-1) \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ A_{p-1} &= 1\cdot 2\cdot 3\cdot\cdots\cdot(p-1). \end{aligned} \tag{5}$$

Ersetzt man nun in der Gleichheit

$$(x+1)(x+2)\cdots(x+p-1) = x^{p-1} + A_1 x^{p-2} + \cdots + A_{p-2}x + A_{p-1}$$

die Unbestimmte x durch $x+1$, so entsteht die andere:

$$\begin{aligned} (x+2)(x+3)\cdots(x+p) = (x+1)^{p-1} &+ A_1(x+1)^{p-2} + \cdots \\ &+ A_{p-2}(x+1) + A_{p-1}, \end{aligned}$$

durch deren Verbindung mit der voraufgehenden die folgende:

$$\begin{aligned} (x+1)^p + A_1(x+1)^{p-1} + \cdots + A_{p-2}(x+1)^2 + A_{p-1}(x+1) \\ = (x+p)\left[x^{p-1} + A_1 x^{p-2} + \cdots + A_{p-2}x + A_{p-1}\right] \end{aligned}$$

hervorgeht; sie führt durch Vergleichung der Koeffizienten gleich hoher Potenzen von x zur Rechten und Linken das nachstehende System von Beziehungen herbei:

$$\begin{aligned} A_1 &= \frac{p(p-1)}{1\cdot 2} \\ 2A_2 &= \frac{p(p-1)(p-2)}{1\cdot 2\cdot 3} + \frac{(p-1)(p-2)}{1\cdot 2}A_1 \\ 3A_3 &= \frac{p(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3\cdot 4} + \frac{(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3}A_1 + \frac{(p-2)(p-3)}{1\cdot 2}A_2 \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ (p-2)A_{p-2} &= p + (p-1)A_1 + (p-2)A_2 + \cdots + 3A_{p-3} \\ (p-1)A_{p-1} &= 1 + A_1 + A_2 + \cdots + A_{p-3} + A_{p-2}. \end{aligned} \tag{6}$$

Werden diese Gleichungen aber als Kongruenzen (mod. p) aufgefafst, so schliefst man nach den Eigenschaften der Binomialkoeffizienten successive, dafs A_1, dann dafs A_2, dann A_3 u. s. w. bis A_{p-2} sämtlich durch p teilbar sind, und infolge davon geht die letzte Gleichung in die Kongruenz:

$$A_{p-1} \equiv -1 \pmod{p} \tag{7}$$

über. Die Gleichheit der beiden Ausdrücke (3) und (4) bedingt mithin die nachfolgende Kongruenz:

$$(8) \qquad (x+1)(x+2)\cdots(x+p-1) \equiv x^{p-1} - 1 \pmod{p}$$

in dem Sinne, dafs die Koeffizienten gleich hoher Potenzen von x zur Rechten und zur Linken (mod. p) kongruent sind; setzt man demnach für die Unbestimmte x irgend welche ganze Zahl, so erhält man rechts und links zwei (mod. p) kongruente Zahlen. Links aber wird je einer der Faktoren und demnach das Produkt durch p teilbar, so oft für x eine der Zahlen $1, 2, \cdots (p-1)$ oder allgemeiner eine Zahl gesetzt wird, die einer von jenen (mod. p) kongruent d. i. welche durch p nicht teilbar ist; und somit geht aus (8) der Fermatsche Satz hervor, dafs für jede durch p nicht teilbare Zahl x

$$x^{p-1} \equiv 1 \pmod{p}$$

sei.

Zugleich aber lehrt die Kongruenz (7) mit Rücksicht auf die letzte der Gleichungen (5) den neuen Satz: dafs, so oft p eine Primzahl ist,

$$(9) \qquad 1 \cdot 2 \cdot 3 \cdots (p-1) \equiv -1 \pmod{p}$$

ist, wofür man auch schreiben kann:

$$(9^a) \qquad 1 \cdot 2 \cdot 3 \cdots (p-1) + 1 \equiv 0 \pmod{p}.$$

Dieser Satz heifst der **Wilson**sche Satz und findet sich zum ersten Mal ausgesprochen bei E. Waring, *medit. algebr.*, Cambridge 1770 (3. éd., p. 380), der ihn, ohne einen Beweis desselben zu bringen, Wilson zuschreibt. Nach Lagrange bewies auch Euler den Satz (*opusc. analyt.*, Petrop. 1773, I p. 329 = *Comm. Ar. coll.* 2, p. 44), sodann Gaufs (*Disqu. Ar. art.* 75—77). Dieser Satz ist besonders dadurch bemerkenswert, dafs er auch umgekehrt werden kann. In der That, wenn p eine zusammengesetzte Zahl wäre, könnte die Kongruenz (9) nicht stattfinden, denn in diesem Falle müfste jeder Primfaktor von p in dem Produkte $1 \cdot 2 \cdot 3 \cdots (p-1)$ auftreten, die linke Seite von (9) also, wie der Modulus, teilbar durch ihn sein, während die rechte Seite es nicht ist. Der Wilsonsche Satz giebt also ein charakteristisches Merkmal für Primzahlen: eine Zahl p ist Primzahl oder nicht, jenachdem die Kongruenz statthat oder nicht. Man könnte ihn daher benutzen, um festzustellen, ob eine gegebene Zahl p Primzahl sei oder nicht; indessen leuchtet sogleich ein, dafs diese Methode ohne praktischen Wert ist, weil die Berechnung des Produktes $1 \cdot 2 \cdot 3 \cdots (p-1)$ sowie auch seines Restes (mod. p) für grofse Zahlen p — und solche kommen zumeist in Frage — bald unausführbar wird.

3. Hat man auf eine der angegebenen Arten den einfachen Fermatschen Satz bewiesen, so gelangt man leicht zu dem verall-

gemeinerten (Eulerschen) Satze (1) wieder zurück. In der That, ist a durch die Primzahl p nicht teilbar, so ist nach jenem Satze

$$a^{p-1} \equiv 1 \pmod{p}$$

d. h.

$$a^{p-1} = 1 + hp,$$

wo h eine ganze Zahl. Wird diese Gleichung nun zur p^{ten} Potenz erhoben, so ergiebt sich nach den Eigenschaften der Binomialkoeffizienten die Kongruenz

$$a^{p(p-1)} \equiv 1 \pmod{p^2}$$

oder die Gleichung

$$a^{p(p-1)} = 1 + h'p^2,$$

wo wieder h' eine ganze Zahl ist. Hieraus folgt

$$a^{p^2(p-1)} = (1 + h'p^2)^p$$

d. i.

$$a^{p^2(p-1)} \equiv 1 \pmod{p^3}$$

u. s. f.; allgemein findet man für jeden positiven ganzen Exponenten α:

$$a^{p^{\alpha-1}(p-1)} \equiv 1 \pmod{p^\alpha},$$

eine Kongruenz, für welche man auch schreiben darf

$$(10) \qquad a^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha}.$$

Gesetzt also, a sei auch durch die Primzahlen $q, r, \ldots$ nicht teilbar, so erhält man gleicherweise für irgend welche positive ganzzahlige Exponenten $\beta, \gamma, \ldots$ die Kongruenzen

$$\begin{aligned} a^{\varphi(q^\beta)} &\equiv 1 \pmod{q^\beta} \\ (10) \qquad a^{\varphi(r^\gamma)} &\equiv 1 \pmod{r^\gamma} \\ &\cdots\cdots \end{aligned}$$

Nun sei, in Primzahlpotenzen zerlegt,

$$n = p^\alpha q^\beta r^\gamma \cdots$$

und a eine zu n prime Zahl. Dann bestehen die sämtlichen Kongruenzen (10); bedeutet daher $\psi(n)$ das kleinste gemeinsame Vielfache der Exponenten $\varphi(p^\alpha)$, $\varphi(q^\beta)$, $\varphi(r^\gamma)$, $\ldots$, so wird offenbar auch jede der Kongruenzen

$$\begin{aligned} a^{\psi(n)} &\equiv 1 \pmod{p^\alpha} \\ a^{\psi(n)} &\equiv 1 \pmod{q^\beta} \\ a^{\psi(n)} &\equiv 1 \pmod{r^\gamma} \\ &\cdots\cdots \end{aligned}$$

und, da deren Moduln relative Primzahlen sind, endlich auch die nachstehende:

$$(11) \qquad a^{\psi(n)} \equiv 1 \pmod{n}$$

erfüllt sein. Hieraus folgt aber, da

$$\varphi(n) = \varphi(p^\alpha)\,\varphi(q^\beta)\,\varphi(r^\gamma)\cdots$$

gewifs ein Vielfaches von $\psi(n)$ ist, auch der verallgemeinerte **Fermat**sche Lehrsatz:

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

so oft a prim ist gegen n.

Setzt man m statt a und schreibt die Kongruenz als Gleichung:

$$m^{\varphi(n)} = 1 + nh,$$

so erkennt man sogleich, dafs der unbestimmten Gleichung

$$mx - ny = 1$$

durch die ganzen Zahlen

$$x = m^{\varphi(n)-1}, \quad y = h$$

Genüge geschieht. Dies gäbe also eine, schon Kap. 4, Ende von Nr. 5 erwähnte neue, doch zumeist praktisch unbrauchbare Methode zur Auflösung dieser Gleichung.

4. Man kann die Frage aufwerfen, ob auch der Fermatsche Satz umgekehrt werden darf und somit, wie der Satz von Wilson, für Primzahlen charakteristisch ist. Diese Frage ist jedoch zu verneinen, wie ein einfaches Beispiel zeigt (s. Lucas, *théor. des nombres*, p. 422). Für den zusammengesetzten Modulus $n = 73 \cdot 37$ bestätigt man bald die beiden Kongruenzen

$$2^{36} \equiv 1 \pmod{37}, \qquad 2^9 \equiv 1 \pmod{73},$$

aus deren letzter umsomehr $2^{36} \equiv 1 \pmod{73}$ und deshalb auch

$$2^{36} \equiv 1 \pmod{n}$$

folgt. Nun ist aber $n - 1 = 36 \cdot 75$, aus der voraufgehenden Kongruenz geht mithin auch die folgende:

$$2^{n-1} \equiv 1 \pmod{n}$$

hervor, also darf man den Schlufs nicht ziehen, dafs, wenn für eine gegen n prime Zahl a die Kongruenz $a^{n-1} \equiv 1 \pmod{n}$ erfüllt ist, n eine Primzahl sei. Gleichwohl läfst sich in geeigneter Weise eine Umkehrung des Fermatschen Satzes formulieren.

Gesetzt nämlich, es sei

$$a^{n-1} \equiv 1 \pmod{n}, \tag{12}$$

so sind zwei Fälle möglich:

entweder ist die $(n-1)^{\text{te}}$ Potenz von a die niedrigste, welche, durch n geteilt, den Rest 1 giebt; dann ersieht man leicht, dafs $n-1$ ein Teiler von $\psi(n)$ und folglich auch von $\varphi(n)$ sein mufs. In der That: andernfalls wäre $\psi(n) = q \cdot (n-1) + r$, wo der Rest r positiv und kleiner als $n - 1$ wäre; also fände man, da gleichzeitig

$$a^{n-1} \equiv 1, \quad a^{\psi(n)} = a^{q(n-1)} \cdot a^r \equiv 1 \pmod{n}$$

ist, auch $a^r \equiv 1 \pmod{n}$ gegen die über $n-1$ gemachte Annahme; hieraus, wie unmittelbar aus der letzteren, folgt dann aber

$$n - 1 \overline{\overline{<}} \varphi(n)$$

oder vielmehr, da $\varphi(n)$ nicht $\overline{\overline{>}} n$ sein kann,

$$n - 1 = \varphi(n),$$

was nur für eine Primzahl n der Fall ist;

oder die $(n-1)^{\text{te}}$ Potenz von a ist nicht die niedrigste, welche, durch n geteilt, den Rest 1 läfst; dann sei a^d diese letztere Potenz; aus dem gleichzeitigen Bestehen der beiden Kongruenzen $a^d \equiv 1$ und $a^{n-1} \equiv 1$ folgt alsdann mittels ähnlicher Schlüsse wie zuvor, dafs d ein Teiler von $n-1$ sein mufs.

Hiernach läfst sich folgender Satz aussprechen (Lucas a. a. O. p. 441), der als die richtige Umkehrung des Fermatschen anzusehen ist: Ist $a^x - 1$ teilbar durch n für $x = n-1$, aber für keinen Wert von x, der in $n-1$ aufgeht, so mufs n eine Primzahl sein.

Z. B. findet man, wenn $a = 3$ und $n = 2^{16} + 1 = 65537$, also die Potenzen

$$1, 2, 2^2, 2^3, \ldots 2^{16}$$

die einzigen Teiler von $n-1$ sind, dafs erst

$$3^{2^{16}} \equiv 1 \pmod{65537}$$

wird; sonach ist 65537 eine Primzahl.

5. Nach dem Fermatschen Satze ist, wenn p eine Primzahl ist, für jede durch p nicht teilbare Zahl a

$$a^{p-1} \equiv 1 \pmod{p}.$$

Jacobi hat (*Journ. f. Math.* 3, 1828, p. 301) zuerst Fälle angegeben, in denen diese Kongruenz für eine der Zahlen $a = 1, 2, \cdots p-1$ auch $(\text{mod.}\, p^2)$ erfüllt ist. Dies führt darauf, den Rest der ganzen Zahl

$$\frac{a^{p-1} - 1}{p}$$

in Bezug auf den Modulus p, oder die durch die Kongruenz

$$a^{p-1} \equiv 1 + p \cdot q(a) \pmod{p^2} \tag{13}$$

für jedes zu p prime a definierte Funktion $q(a) \pmod{p}$ zu untersuchen. Eisenstein hat solche Untersuchung begonnen (*Berl. Monatsber.* 1850, p. 41), später folgten ihm Stern (*Journ. f. Math.* 100, 1887, p. 182) und Mirimanoff (ebendas. 115, 1895, p. 295), nachdem schon Sylvester (*Par. C. R.* 52, 1861, p. 161) eine Reihe bezüglicher, teilweise der Verbesserung bedürftiger Sätze angegeben hatte.

Zunächst ist offenbar, dafs $q(a) \pmod{p}$ ungeändert bleibt, wenn a durch eine $(\text{mod.}\, p^2)$ kongruente Zahl ersetzt wird, in Zeichen:

$$q(a + p^2 z) \equiv q(a) \pmod{p}. \tag{14}$$

Da ferner

$$(a+pz)^{p-1} \equiv a^{p-1} + (p-1)pa^{p-2}z$$

$$\text{d. i.} \quad \equiv a^{p-1} - p \cdot \frac{z}{a} \cdot a^{p-1} \pmod{p^2}$$

ist, wo man $\frac{1}{a}$ durch den socius von a ersetzt zu denken hat, so findet sich wegen (13)

$$(a+pz)^{p-1} \equiv 1 + p\left(q(a) - \frac{z}{a}\right) \pmod{p^2}$$

d. i.

$$q(a+pz) \equiv q(a) - \frac{z}{a} \pmod{p}. \tag{15}$$

Ist ferner auch b eine durch p nicht teilbare Zahl, sodaſs

$$b^{p-1} \equiv 1 + p \cdot q(b) \pmod{p^2}$$

zu setzen ist, so findet man

$$(ab)^{p-1} \equiv 1 + p(q(a) + q(b)) \pmod{p^2}$$

und folglich

$$q(ab) \equiv q(a) + q(b) \pmod{p}. \tag{16}$$

Die letzten beiden Formeln (15), (16) gestatten, um allgemein $q(a)$ zu finden, sich, wenn man will, auf solche Argumente a zu beschränken, welche Primzahlen $< p$ sind.

Bevor zu solcher Bestimmung weiter fortgeschritten werden soll, sei bemerkt, daſs zum Stattfinden der Kongruenz

$$a^{p-1} \equiv 1 \pmod{p^2}$$

offenbar die Bedingung $q(a) \equiv 0 \pmod{p}$ notwendig und hinreichend ist. Um daher sämtliche vorhandenen Wurzeln der Kongruenz

$$x^{p-1} \equiv 1 \pmod{p^2} \tag{17}$$

zu finden, setze man $x \equiv a + pz \pmod{p^2}$, wo a irgend eine der Zahlen $1, 2, 3, \cdots (p-1)$ bedeutet; soll eine solche Zahl x der Kongruenz genügen, so muſs

$$q(x) \equiv q(a+pz) \equiv q(a) - \frac{z}{a} \equiv 0 \pmod{p}$$

d. i. $z \equiv aq(a) \pmod{p}$ und folglich

$$x \equiv a + pa \cdot q(a) \pmod{p^2} \tag{18}$$

sein. Ist umgekehrt x eine Zahl dieser Form, so folgt

$$x^{p-1} \equiv a^{p-1} + p(p-1)a^{p-1} \cdot q(a) \pmod{p^2}$$

d. i. wegen (13) einfacher

$$x^{p-1} \equiv 1 + p \cdot q(a) - p \cdot q(a)(1 + p \cdot q(a)) \equiv 1 \pmod{p^2}.$$

Somit giebt die Formel (18) sämtliche Wurzeln der Kongruenz (17), wenn man für a sämtliche Zahlen $1, 2, 3, \cdots (p-1)$ setzt. Diejenigen a, für welche $q(a) \equiv 0 \pmod{p}$, liefern die von

Jacobi betrachteten Fälle; bis zur Primzahl 37 hin finden sich so die Fälle:

$$p = 11, \quad a = 3,9$$
$$p = 29, \quad a = 14$$
$$p = 37, \quad a = 18.$$

Wir gehen nun aus von der Binomialentwicklung

$$(19) \quad (1+u)^p = 1 + \frac{p}{1} u + \frac{p(p-1)}{1 \cdot 2} u^2 + \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3} u^3 + \cdots + \frac{p(p-1)(p-2)\cdots(p-(p-2))}{1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1)} u^{p-1} + u^p.$$

Versteht man auch ferner allgemein unter $\frac{1}{m}$ den socius von m (mod. p), so läfst sich die vorige Gleichung als Kongruenz (mod. p^2) folgendermafsen schreiben:

$$(1+u)^p \equiv 1 + pu - \frac{pu^2}{2} + \frac{pu^3}{3} - \cdots - \frac{p \cdot u^{p-1}}{p-1} + u^p \pmod{p^2},$$

woraus sich dann ergiebt

$$(20) \quad \frac{(1+u)^p - (1+u)}{p} \equiv u - \frac{u^2}{2} + \frac{u^3}{3} - \cdots - \frac{u^{p-1}}{p-1} + \frac{u^p - u}{p} \pmod{p}.$$

Setzt man in dieser Kongruenz für u der Reihe nach $1, 2, 3, \cdots (a-1)$ ein und addiert die so entstehenden Kongruenzen, so erhält man

$$(21) \quad \frac{a^p - a}{p}$$
$$\equiv S_1(a-1) - \frac{1}{2} S_2(a-1) + \frac{1}{3} S_3(a-1) \cdots - \frac{1}{p-1} S_{p-1}(a-1) \pmod{p},$$

wenn unter $S_k(a-1)$ die Summe der k^{ten} Potenzen der Zahlen $1, 2, 3, \cdots (a-1)$ verstanden, also

$$(22) \quad S_k(a-1) = 1^k + 2^k + 3^k + \cdots + (a-1)^k$$

gesetzt wird. Diese Formel gestattet, jederzeit die Funktion $q(a)$ zu berechnen, denn offenbar ist

$$(23) \quad \frac{a^p - a}{p} \equiv a \cdot q(a) \pmod{p}.$$

Eine zweite, ähnliche Formel erhält man ausgehend von der Entwicklung

$$(u-1)^p = u^p - \frac{p}{1} u^{p-1} + \frac{p(p-1)}{1 \cdot 2} u^{p-2} - \cdots - 1,$$

welche (mod. p^2) aufgefafst, zu der folgenden Kongruenz führt:

$$(24) \quad \frac{(u-1)^p - (u-1)}{p} \equiv \frac{u^p - u}{p} - \left(u^{p-1} + \frac{u^{p-2}}{2} + \cdots + \frac{u}{p-1}\right) \pmod{p}$$

und, indem man hierin u successive gleich $1, 2, 3, \ldots a$ setzt, die Formel:

$$(25)\qquad \frac{a^p - a}{p} \equiv S_{p-1}(a) + \frac{1}{2} S_{p-2}(a) + \cdots + \frac{1}{p-1} S_1(a) \pmod{p}$$

erschliefsen läfst.

6. Besonders einfache und bemerkenswerte Beziehungen ergeben sich aus diesen allgemeinen Formeln, wenn $a = 2$ gewählt wird. Um sie zu erhalten, schicken wir zwei einfache Bemerkungen vorauf.

Da $\frac{1}{m}$ die Zahl x ist, welche der Kongruenz $mx \equiv 1 \pmod{p}$ genügt, und $\frac{1}{p-m}$ die Zahl y, für welche $(p-m)y \equiv 1 \pmod{p}$ ist, so zeigt sich sogleich durch Addition und Subtraktion dieser beiden Kongruenzen, dafs

$$(26)\qquad m(x-y) \equiv 2, \quad m(x+y) \equiv 0 \pmod{p}$$

ist, Kongruenzen, aus deren zweiter die Beziehung

$$(27)\qquad \frac{1}{m} + \frac{1}{p-m} \equiv 0 \pmod{p}$$

hervorgeht. Setzt man hierin für m der Reihe nach $1, 2, 3, \cdots \frac{p-1}{2}$ und addiert die Resultate, so findet man die Formel

$$(28)\qquad 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p},$$

die übrigens auch aus (24) entsteht, wenn $u = 1$ gesetzt wird. Ferner läfst sich die erste der Kongruenzen (26), jenachdem m ungerade oder gerade ist, folgendermafsen schreiben:

$$\left.\begin{aligned} \frac{p+m}{2}(x-y) &\equiv 1 \\ \left(p - \frac{m}{2}\right)(y-x) &\equiv 1 \end{aligned}\right\} \pmod{p}$$

und ergiebt entsprechend:

$$(29)\qquad \begin{aligned} &(m \text{ ungerade}) \qquad \frac{1}{m} - \frac{1}{p-m} \equiv \frac{1}{\frac{p+m}{2}}, \\ &(m \text{ gerade}) \qquad -\frac{1}{m} + \frac{1}{p-m} \equiv \frac{1}{p-\frac{m}{2}}. \end{aligned}$$

In Anwendung dieser Resultate auf den Ausdruck

$$(30)\qquad 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{1}{p-2} - \frac{1}{p-1}$$

findet sich zuerst für den Fall, dafs $p = 4z + 1$ ist, durch Addition der Formeln (29) für $m = 1, 3, \cdots \frac{p-3}{2}$, resp. für $m = 2, 4, \cdots \frac{p-1}{2}$, dafs jener Ausdruck (mod. p) dem folgenden:

$$\frac{1}{\frac{p+1}{2}} + \frac{1}{\frac{p+3}{2}} + \cdots + \frac{1}{p-1}$$

kongruent ist. Dasselbe findet sich, falls $p = 4z + 3$ ist, wenn man die Formeln (29) für $m = 1, 3, \cdots \frac{p-1}{2}$, resp. für $m = 2, 4, \cdots \frac{p-3}{2}$ bildet und die Resultate addiert. Auf solche Weise gelangt man also allgemein zu der ferneren Beziehung:

$$(31)\quad 1 - \frac{1}{2} + \frac{1}{3} \cdots - \frac{1}{p-1} \equiv \frac{1}{\frac{p+1}{2}} + \frac{1}{\frac{p+3}{2}} + \cdots + \frac{1}{p-1} \pmod{p}.$$

Leicht aber überzeugt man sich, dafs in der letzteren die Kongruenz sogar durch Gleichheit ersetzt werden kann. Denn, addiert man zur Gleichheit

$$1 - \frac{1}{2} = \frac{1}{2}$$

beiderseits $\frac{1}{3} - \frac{1}{4}$, so kommt zunächst

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} = \frac{1}{3} + \frac{1}{4};$$

hieraus folgt

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} = \frac{1}{4} + \frac{1}{5} + \frac{1}{6},$$

ferner

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \frac{1}{7} - \frac{1}{8} = \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}$$

u. s. w., bis man zur Gleichheit

$$(32)\quad 1 - \frac{1}{2} + \frac{1}{3} \cdots - \frac{1}{p-1} = \frac{1}{\frac{p+1}{2}} + \frac{1}{\frac{p+3}{2}} + \cdots + \frac{1}{p-1}$$

gelangt, die hiermit sogar allgemeiner, als die Kongruenz, für jede ungerade Zahl p als giltig erwiesen ist.

Nunmehr fliefst zunächst unmittelbar aus (21) für $a = 2$ die Beziehung:

$$(33)\quad \frac{2^p - 2}{p} \equiv 1 - \frac{1}{2} + \frac{1}{3} - \cdots - \frac{1}{p-1} \pmod{p},$$

welcher man der letzten Formel zufolge auch die Gestalt geben kann:

$$(34)\quad \frac{2^p - 2}{p} \equiv \frac{1}{\frac{p+1}{2}} + \frac{1}{\frac{p+3}{2}} + \cdots + \frac{1}{p-1} \pmod{p},$$

eine Beziehung, von welcher wir bereits am Schlusse des vorigen Kapitels Gebrauch gemacht haben. Addiert man aber zu (33) die Kongruenz (28), so ergiebt sich die Formel

$$(35)\qquad \frac{2^{p-1}-1}{p} \equiv 1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p-2} \pmod{p},$$

welche unmittelbar die Funktion $q(2) \pmod{p}$ berechnen lehrt.

Sylvester hat a. a. O. noch andere Ausdrücke für denselben Quotienten gegeben, zu denen man nach Stern's Vorgange durch die Binomialentwicklung für $(1+i)^{2p}$, wo $i=\sqrt{-1}$ gedacht ist, gelangen kann. Man findet nämlich zunächst

$$\frac{(1+i)^{2p}-1-i^{2p}}{p} \equiv 2i - \frac{2i^2}{2} + \frac{2i^3}{3} \cdots - \frac{2i^{2p-2}}{2} + 2i^{2p-1} \pmod{p}.$$

Nun heben sich aber rechts je zwei Glieder mit geraden Exponenten, wie $\frac{2i^2}{2}, \frac{2i^{2p-2}}{2}$ gegenseitig auf, während je zwei Glieder mit ungeraden Exponenten, wie $2i$ und $2i^{2p-1}$ einander gleich sind, sodaſs sich

$$\frac{(1+i)^{2p}-1-i^{2p}-2i^p}{p} \equiv 2\cdot 2i\left(1-\frac{1}{3}+\frac{1}{5}\cdots \mp \frac{1}{p-2}\right) \pmod{p}$$

ergiebt, wo das obere oder untere Vorzeichen gilt, jenachdem p gleich $4z+1$ oder gleich $4z+3$ ist. Da aber je nach diesen Fällen

$$(1+i)^{2p}-1-i^{2p}-2i^p = \pm 2i(2^{p-1}-1)$$

gefunden wird, so darf man schreiben:

$$(36)\qquad \pm\frac{2^{p-1}-1}{p} \equiv 2\left(1-\frac{1}{3}+\frac{1}{5}-\cdots \mp \frac{1}{p-2}\right) \pmod{p};$$

die oberen und unteren Vorzeichen rechts und links korrespondieren. Unterscheidet man hier die beiden Fälle $p=4z+1$ und $p=4z+3$, denen sie resp. entsprechen, so kann man noch andere Ausdrücke für $q(2)$ herleiten, wie wenigstens für den ersteren Fall noch gezeigt werden mag. Wird in diesem die doppelt genommene Kongruenz (28) zu (36) addiert, so kommt

$$\frac{2^{p-1}-1}{p} \equiv 2\left(\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{p-1}\right) + 4\left(1+\frac{1}{5}+\cdots+\frac{1}{p-4}\right);$$

da aber nach (27)

$$1+\frac{1}{p-1}\equiv 0, \qquad \frac{1}{5}+\frac{1}{p-5}\equiv 0, \cdots$$

ist, so erhält die vorige Kongruenz die einfachere Gestalt:

$$(37)\ \frac{2^{p-1}-1}{p} \equiv 2\left(\frac{1}{p-3}+\frac{1}{p-4}+\frac{1}{p-7}+\frac{1}{p-8}+\cdots+\frac{1}{6}+\frac{1}{5}+\frac{1}{2}+1\right) \pmod{p},$$

in welcher sie von Sylvester angegeben worden ist. Ein anderer, von demselben Mathematiker, aber ungenau mitgeteilter Ausdruck ergiebt sich aus (33), wenn man bedenkt, daſs

$$1+\frac{1}{p-1}\equiv 0, \quad \frac{1}{2}+\frac{1}{p-2}\equiv 0, \cdots$$

ist; so geht nämlich daraus die Kongruenz

$$\frac{2^{p-1}-1}{p}\equiv -\frac{1}{p-1}+\frac{1}{p-2}-\cdots\pm\frac{1}{\frac{p+1}{2}} \tag{38}$$

hervor, in welcher wieder das obere oder untere Vorzeichen zu nehmen ist, jenachdem $p=4z+1$ oder $p=4z+3$ ist.

7. Die allgemeinen Ausdrücke, welche Mirimanoff für die Funktion $q(a)$ gegeben hat, sind von den vorher ermittelten sehr verschieden und fliefsen auch aus einer durchaus anderen Quelle als sie.

Wir bemerken zuvörderst, dafs es nach dem Fermatschen Satze für jede nicht durch p teilbare Zahl a eine Potenz giebt, welche, durch p geteilt, den Rest 1 läfst. Ist die $(p-1)^{\text{te}}$ Potenz die niedrigste Potenz dieser Art, so nennt man a eine primitive Wurzel (mod. p); andernfalls sei a^d diese niedrigste Potenz; man überzeugt sich dann aus dem gleichzeitigen Stattfinden der beiden Kongruenzen

$$a^{p-1}\equiv 1, \quad a^d\equiv 1 \pmod{p},$$

wie in Nr. 4, dafs d ein Teiler von $p-1$, also $\frac{p-1}{d}=e$ eine ganze Zahl ist; den Exponenten d nennt man den Exponenten, zu welchem a (mod. p) gehört; jede primitive Wurzel (mod. p) gehört mithin zum Exponenten $p-1$. Der Grundeigenschaften der Funktion $q(a)$ wegen dürfen wir uns, wie schon bemerkt, auf den Fall beschränken, dafs a eine Primzahl $<p$ sei, und wir halten diese Annahme im Folgenden fest.

Dies voraufgeschickt, betrachte man den Quotienten $\frac{a^d-1}{p}$, welcher, als eine Zahl im Ziffernsysteme mit der Basis a dargestellt, die Form

$$\frac{a^d-1}{p}=\alpha_0+\alpha_1 a^{k_1}+\alpha_2 a^{k_2}+\cdots+\alpha_n a^{k_n} \tag{39}$$

haben wird, wo die Koeffizienten $\alpha_0, \alpha_1, \alpha_2, \ldots \alpha_n$ Zahlen der Reihe $1, 2, 3, \ldots (a-1)$ sind, die Exponenten aber wachsende positive ganze Zahlen bedeuten, sodafs

$$k_1<k_2<\cdots<k_n<d.$$

Aus der aufgestellten Formel zieht man zunächst den Schlufs:

$$\alpha_0 p+1=a^{k_1}\cdot\beta_1,$$

wo β_1 eine positive, zu a prime ganze Zahl bezeichnet; da die Kongruenz

$$xp+1\equiv 0 \pmod{a} \tag{40}$$

nur eine einzige Wurzel hat, ist offenbar α_0 der kleinste positive Rest dieser Wurzel. Nun ergiebt sich aus (39) ferner:

$$a^{d-k_1} = \beta_1 + p\alpha_1 + p(\alpha_2 a^{k_2-k_1} + \cdots + \alpha_n a^{k_n-k_1}) \tag{41}$$

und folglich

$$\alpha_1 p + \beta_1 = a^{k_2-k_1} \cdot \beta_2,$$

wo wieder β_2 eine positive, zu a prime ganze Zahl bedeutet und α_1 der kleinste positive Rest der Wurzel der Kongruenz

$$xp + \beta_1 \equiv 0 \pmod{a}$$

ist. Die Gleichung (41) geht dadurch über in die folgende:

$$a^{d-k_2} = \beta_2 + p\alpha_2 + p(\alpha_3 a^{k_3-k_2} + \cdots + \alpha_n a^{k_n-k_2})$$

und liefert eine neue Gleichung

$$\alpha_2 p + \beta_2 = a^{k_3-k_2} \cdot \beta_3$$

u. s. w., bis man auf eine letzte Gleichung dieser Art:

$$\alpha_n p + \beta_n = a^{d-k_n} \cdot 1$$

geführt wird. Setzt man also noch

$$e_0 = k_1, \quad e_1 = k_2 - k_1, \quad e_2 = k_3 - k_2, \cdots, e_n = d - k_n, \tag{42}$$

sodafs

$$e_0 + e_1 + e_2 + \cdots + e_n = d \tag{43}$$

wird, so zieht man aus der Gleichung (39) nachstehendes System von Gleichungen:

$$\begin{aligned} \alpha_0 p + 1 &= a^{e_0} \cdot \beta_1, \\ \alpha_1 p + \beta_1 &= a^{e_1} \cdot \beta_2, \\ &\cdots\cdots \\ \alpha_i p + \beta_i &= a^{e_i} \cdot \beta_{i+1}, \\ &\cdots\cdots \\ \alpha_n p + \beta_n &= a^{e_n} \cdot 1, \end{aligned} \tag{44}$$

welches man auch direkt aufstellen kann, wenn man, ausgehend von der Kongruenz (40), allgemein mit α_i den kleinsten positiven Rest der Wurzel der Kongruenz

$$xp + \beta_i \equiv 0 \pmod{a} \tag{45}$$

und mit β_{i+1} den Quotienten aus $\alpha_i p + \beta_i$ und der höchsten darin aufgehenden Potenz von a, unter β_0 endlich die 1 versteht. Hiernach sind die Zahlen $1, \beta_1, \beta_2, \ldots \beta_n$ positiv, prim gegen a, und auch kleiner als p; denn, gilt letzteres schon von β_i, so folgt

$$a^{e_i}\beta_{i+1} = \alpha_i p + \beta_i \overline{\overline{<}} (a-1)p + p - 1 < ap,$$

umsomehr also auch $\beta_{i+1} < p$; da nun $\beta_0 = 1 < p$, so folgt $\beta_1 < p$, also auch $\beta_2 < p$, u. s. w. fort. Man schliefst ferner aus den Gleichungen (44) die Kongruenzen

$$a^{e_0} \cdot \beta_1 \equiv 1, \quad a^{e_0+e_1} \cdot \beta_2 \equiv 1, \ldots, a^{e_0+e_1+\cdots+e_i} \cdot \beta_{i+1} \equiv 1, \ldots \pmod{p}$$

und demnach haben die Zahlen $1, \beta_1, \beta_2, \ldots \beta_n$ noch die weitere Eigenschaft, dafs für jede derselben eine Kongruenz $a^h \cdot \beta_i \equiv 1$ oder auch, indem man $d - h = k$ setzt, eine Kongruenz $\beta_i \equiv a^k \pmod{p}$ erfüllt ist. Sie sind daher auch verschieden.

Wir zeigen endlich, dafs die Zahlen $1, \beta_1, \beta_2, \ldots \beta_n$ auch jede positive, zu a prime Zahl $\beta < p$, welche einer Potenz von a kongruent ist (mod. p), unter sich enthalten. In der That, sei $\beta \equiv a^k$ oder $a^h \beta \equiv 1 \pmod{p}$, so kann man schreiben:

$$a^h \beta = 1 + pN,$$

wo N eine durch a nicht teilbare ganze Zahl $\gtreqless 0$ bedeutet; für $N = 0$ würde, die Behauptung bestätigend, $\beta = 1$. Sei also $N > 0$, n_0 der kleinste positive Rest von $N \pmod{a}$; dann kann man setzen:

$$a^h \beta = 1 + pn_0 + pa^{m_1} N_1,$$

wo die ganze Zahl $N_1 \gtreqless 0$ und durch a nicht teilbar ist. Da hiernach $1 + pn_0$ durch a aufgeht, mufs $n_0 = \alpha_0$, $1 + pn_0 = a^{e_0} \cdot \beta_1$ sein, und die vorige Gleichung nimmt die Gestalt an:

$$a^h \beta = a^{e_0} \beta_1 + pa^{m_1} N_1.$$

Wäre $N_1 = 0$, so ergäbe sich $h = e_0$, $\beta = \beta_1$, der Behauptung entsprechend. Man nehme also N_1 positiv an. Dann kann h nicht $< e_0$ sein, denn sonst wäre — was alles gegen die Voraussetzungen ist — β durch a teilbar, oder $> p$, oder N_1 teilbar durch a, jenachdem $h < m_1$, $h = m_1$, $h > m_1$ gedacht wird. Ebensowenig kann $h = e_0$ sein, da sonst $m_1 \gtreqless h$ sein müfste, womit $\beta > p$ würde. Ist demnach $h > e_0$, so mufs, da β_1 prim gegen a ist, $m_1 = e_0$ sein und die obige Gleichung nimmt die Gestalt an:

$$a^{h-e_0} \cdot \beta = \beta_1 + pN_1,$$

und giebt, falls n_1 der kleinste positive Rest von $N_1 \pmod{a}$ ist, die andere:

$$a^{h-e_0} \cdot \beta = \beta_1 + pn_1 + pa^{m_2} \cdot N_2,$$

unter N_2 wieder eine ganze Zahl $\gtreqless 0$ verstanden, welche prim ist gegen a. Aus letzterer Gleichung schliefst man nun genau wie zuvor, dafs $n_1 = \alpha_1$, also $\beta_1 + pn_1 = a^{e_1} \cdot \beta_2$ und entweder $h - e_0 = e_1$ d. h. $h = e_0 + e_1$ und $\beta = \beta_2$ ist, wie es der Behauptung entspricht, oder dafs $h > e_0 + e_1$ sein mufs, in welchem Falle dann die Betrachtung in gleicher Weise fortgesetzt werden kann. Da aber die Reihe der Zahlen e_0, $e_0 + e_1$, $e_0 + e_1 + e_2, \ldots$ bis zur Zahl

$$e_0 + e_1 + e_2 + \cdots + e_n = d$$

aufsteigt, welche $\gtreqless h$ ist, so mufs endlich β mit einer der Zahlen $1, \beta_1, \beta_2, \ldots \beta_n$ identisch sich ergeben, w. z. b. w.

Nach Feststellung dieser Eigenschaften der letzteren Zahlen bemerke man nun, daſs nach (15)

$$q(\alpha_i p + \beta_i) \equiv q(\beta_i) - \frac{\alpha_i}{\beta_i} \pmod{p}$$

und nach (16)

$$q(a^{e_i} \cdot \beta_{i+1}) \equiv e_i \cdot q(a) + q(\beta_{i+1}) \pmod{p}$$

ist; wegen (44) also ergiebt sich

$$q(\beta_i) - \frac{\alpha_i}{\beta_i} \equiv e_i \cdot q(a) + q(\beta_{i+1}) \pmod{p},$$

und, wenn diese Gleichung für alle Werte des Index $i = 0, 1, 2, \ldots n$ gebildet und die entstehenden Formeln addiert werden, mit Rücksicht auf den evidenten Wert

$$q(\beta_0) = q(\beta_{n+1}) = q(1) = 0$$

die folgende Kongruenz:

$$-\sum_{i=0}^{n} \frac{\alpha_i}{\beta_i} \equiv q(a) \cdot \sum_{i=0}^{n} e_i$$

oder wegen (43) und da $de = p - 1 \equiv -1 \pmod{p}$ ist, diese andere:

$$q(a) \equiv e \cdot \sum_{i=0}^{n} \frac{\alpha_i}{\beta_i}, \tag{46}$$

in welcher die Summation auf alle Zahlen β_i, d. h. auf alle Zahlen der Reihe $1, 2, 3, \ldots p-1$ zu erstrecken ist, welche prim gegen a und einer Potenz von $a \pmod{p}$ kongruent sind, während dann α_i jedesmal der kleinste positive Rest der Wurzel der Kongruenz (45) ist.

Man findet z. B., wenn $p = 13$, $a = 3$ gewählt wird, $d = 3$, $e = 4$; ferner ist bereits

$$2 \cdot 13 + 1 = 3^3 \cdot 1,$$

also reduziert sich die Reihe der Zahlen $1, \beta_1, \ldots \beta_n$ auf die erste derselben $\beta_0 = 1$, welcher $\alpha_0 = 2$ entspricht; nach (46) ist mithin

$$q(3) \equiv 4 \cdot \frac{2}{1} \equiv 8 \pmod{13}.$$

In der That ist $3^{12} - 1 = 531440$ und

$$\frac{3^{12} - 1}{13} = 40880 \equiv 8 \pmod{13}.$$

Wählt man dagegen $p = 23$, $a = 2$, so ist $d = 11$, $e = 2$, die Reihe der Gleichungen (44) wird diese:

$$1 \cdot 23 + 1 = 2^3 \cdot 3,$$
$$1 \cdot 23 + 3 = 2^1 \cdot 13,$$
$$1 \cdot 23 + 13 = 2^2 \cdot 9,$$
$$1 \cdot 23 + 9 = 2^5 \cdot 1,$$

ferner ergeben sich die Werte

$$\frac{1}{3} \equiv 8, \quad \frac{1}{13} \equiv 16, \quad \frac{1}{9} \equiv 18 \equiv 64 \pmod{23},$$

mithin nach (46)

$$q(2) \equiv 2\left(1 + \frac{1}{3} + \frac{1}{13} + \frac{1}{9}\right)$$
$$\equiv 2(1 + 8 + 16 + 64) \equiv 2 \cdot 89 \equiv 17;$$

in der That ist $2^{22} - 1 = 4194303$ also

$$\frac{2^{22} - 1}{23} = 182361 \equiv 17 \pmod{23}.$$

Ist $d = p - 1$, also a primitive Wurzel (mod. p), so ist, wie später gezeigt werden wird, jede der Zahlen $1, 2, 3, \ldots p - 1$ einer Potenz von a (mod. p) kongruent. In diesem Falle erstreckt sich also die Summation in der Formel (46) auf **alle** Zahlen der Reihe $1, 2, 3, \ldots p - 1$, welche prim sind zu a. Man darf sogar, wenn man will, sie auf die ganze Reihe dieser Zahlen ausdehnen, da, so oft β_i eine durch a teilbare Zahl der Reihe $1, 2, 3, \ldots p-1$ bedeutet, die kleinste Zahl α_i, für welche $\alpha_i p + \beta_i \equiv 0$ (mod. a) wird, $\alpha_i = 0$ ist, das entsprechende Glied der Summe (46) also verschwindet.

Insbesondere nimmt hiernach die Formel (46) in dem Falle, wo $a = 2$ eine primitive Wurzel (mod. p) ist, die Gestalt an:

$$q(2) \equiv 1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p-2} \pmod{p}. \tag{47}$$

Dies ist z. B. der Fall für $p = 11$, wo dann

$$\frac{1}{3} \equiv 4, \quad \frac{1}{5} \equiv 9, \quad \frac{1}{7} \equiv 8, \quad \frac{1}{9} \equiv 5 \pmod{11}$$

also

$$q(2) \equiv 1 + 4 + 9 + 8 + 5 \equiv 5 \pmod{11}$$

gefunden wird, und in der That ist

$$2^{10} - 1 = 1023 \quad \text{also} \quad \frac{2^{10} - 1}{11} = 93 \equiv 5 \pmod{11}.$$

Man sieht, dafs die Formel (47) durchaus mit der früher nach Stern hergeleiteten Formel (35) übereinkommt; aber es ist bemerkenswert, dafs wir sie aus der Mirimanoff'schen Formel (46) nur unter der Voraussetzung gewannen, dafs 2 eine primitive Wurzel (mod. p) sei. —

8. Wir knüpfen nun wieder an den Wilsonschen Satz an. Gaufs hat zwei Beweise desselben gegeben; den ersteren, der aus der allgemeinen Theorie der binomischen Kongruenzen fliefst (*Disqu. Ar. art.* 76), berühren wir später (Kap. 7, Nr. 7); der zweite, sehr einfache Beweis (*art.* 77) beruht auf der Theorie der „associierten Zahlen (socii)“, die Gaufs auch dazu geführt hat, diejenige Verallgemeinerung des Satzes zu geben, in welcher er für jedweden Modulus giltig ist. Der so verallgemeinerte **Wilsonsche** Satz sagt aus: Das Produkt der Zahlen, welche $< n$ und prim gegen n sind (allgemeiner: das Produkt aller Zahlen, die ein reduziertes Restsystem (mod. n) bilden), ist kongruent -1 (mod. n), wenn $n = 4$ oder eine Primzahlpotenz p^a oder das Doppelte einer solchen, $2p^a$, ist, in jedem andern Falle ist es kongruent $+1$ (mod. n). (Gaufs, *D. A. art.* 78). Nach den Gaufsschen Andeutungen ist der erste Beweis dieses allgemeineren Lehrsatzes von Brennecke (*Journ. f. Math.* 19, 1839, p. 319) geliefert worden (s. auch A. L. Crelle, ebend. 20, 1840, p. 29); in ähnlicher Weise wie Jener gab ihn später E. Schering (*Acta Math.* 1, 1883, p. 153).

Man bedarf für die Gaufsche Beweismethode einer vorläufigen Untersuchung über die Anzahl der Wurzeln, welche die quadratische Kongruenz

$$x^2 \equiv 1 \pmod{n} \tag{48}$$

zuläfst; nennen wir sie $\chi(n)$. Eine Wurzel hat diese Kongruenz augenscheinlich immer, nämlich die Wurzel $x \equiv 1$ (mod. n). Um $\chi(n)$ allgemein zu bestimmen, unterscheiden wir verschiedene Fälle.

1) Sei $n = p^a$, Potenz einer ungeraden Primzahl p. Soll nun $x^2 \equiv 1$ (mod. p^a) d. h. $x^2 - 1 = (x+1)(x-1)$ teilbar sein durch p^a, so müssen sich die a Faktoren p so auf die beiden Faktoren $x+1$ und $x-1$ verteilen, dafs deren Produkt sie sämtlich enthält; aber gleichzeitig können $x+1$, $x-1$ nicht durch p aufgehen, da die Differenz 2 dieser Ausdrücke es nicht thut, also mufs entweder $x-1$ oder $x+1$ durch p^a aufgehen, und somit findet man für die Kongruenz

$$x^2 \equiv 1 \pmod{p^a} \tag{49}$$

nur die zwei Wurzeln

$$x \equiv 1 \pmod{p^a}; \quad x \equiv -1 \pmod{p^a} \tag{49^a}$$

folglich

$$\chi(p^a) = 2. \tag{49^b}$$

2) Ist $n = 2$, so wird die Kongruenz

$$x^2 \equiv 1 \pmod{2} \tag{50}$$

durch keine gerade, aber durch jede ungerade Zahl erfüllt, welche Zahlen nur die einzige Wurzel

$$x \equiv 1 \pmod{2} \tag{50^a}$$

bilden, man hat mithin

$$\chi(2) = 1. \tag{50^b}$$

3) Ist dagegen $n = 4$, so wird zwar wieder die Kongruenz

$$x^2 \equiv 1 \pmod{4} \tag{51}$$

durch keine gerade, dagegen durch jede ungerade Zahl erfüllt, da für $x = 2z + 1$ sich $x^2 = 4z^2 + 4z + 1 \equiv 1 \pmod{4}$ ergiebt, aber die letzteren haben entweder die Form $4z + 1$ oder $4z + 3$, bilden mithin zwei Wurzeln:

$$x \equiv 1 \pmod{4}; \quad x \equiv 3 \pmod{4} \tag{51^a}$$

und man findet

$$\chi(4) = 2. \tag{51^b}$$

4) Ist ferner $n = 2^k$, $k \geqq 3$, so müssen, damit

$$x^2 \equiv 1 \pmod{2^k} \tag{52}$$

oder $x^2 - 1 = (x-1)(x+1)$ durch 2^k teilbar sei, die k Faktoren 2 sich auf die beiden Faktoren $x - 1$, $x + 1$ verteilen; da aber deren Differenz gleich 2 ist, so müssen beide Faktoren gerade, einer von ihnen durch 2^1, der andere durch 2^{k-1} teilbar sein, entweder ist demnach $x = 1 + 2^{k-1}y$ oder $x = -1 + 2^{k-1}y$, daraus folgen aber, da y gerade oder ungerade sein kann, vier Wurzeln der Kongruenz:

$$\begin{aligned} x &\equiv 1 \pmod{2^k}; \quad &x &\equiv -1 \pmod{2^k}; \\ x &\equiv 1 + 2^{k-1} \pmod{2^k}; \quad &x &\equiv -1 - 2^{k-1} \pmod{2^k}; \end{aligned} \tag{52^a}$$

mithin ist:

$$\chi(2^k) = 4. \tag{52^b}$$

5) Wenn endlich n eine beliebige ganze Zahl, also

$$n = 2^k p^a q^b r^c \ldots \tag{53}$$

ist, wo $p, q, r, \ldots$ verschiedene ungerade Primzahlen, $a, b, c, \ldots$ positive ganze Zahlen, k Null oder eine positive ganze Zahl bedeuten, so kann

$$x^2 \equiv 1 \pmod{n} \tag{54}$$

nur statthaben, wenn x jede der einfacheren Kongruenzen:

$$x^2 \equiv 1 \pmod{2^k} \tag{55}$$

— wenn $k = 0$ ist, fällt diese Kongruenz fort —

$$\begin{aligned} x^2 &\equiv 1 \pmod{p^a}, \\ x^2 &\equiv 1 \pmod{q^b}, \\ &\cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \end{aligned} \tag{55}$$

erfüllt; aus jeder Lösung $x \equiv \xi \pmod{n}$ von (54) ergiebt sich also

$$\xi \equiv \lambda \pmod{2^k}, \quad \xi \equiv \alpha \pmod{p^a}, \quad \xi \equiv \beta \pmod{q^b}, \ldots, \tag{56}$$

wo $\lambda, \alpha, \beta, \ldots$ je eine Wurzel der Kongruenzen (55) bezeichnen. Bestimmt man umgekehrt für irgend eine Kombination solcher Wurzeln $\lambda, \alpha, \beta, \ldots$ eine Zahl ξ durch die Kongruenzen (56), was, da die Moduln der letzteren zu je zweien relativ prim sind, nach Kap. 3, Nr. 8 eindeutig geschehen kann, so bestehen für $x = \xi$ gleichzeitig die Kongruenzen (55) und folglich wird auch die Kongruenz (54) erfüllt. Da endlich die durch (56) für verschiedene Kombinationen von Wurzeln $\lambda, \alpha, \beta, \ldots$ bestimmten ξ nach der eben angeführten Stelle (mod. n) inkongruente Werte sind, so hat ersichtlich die Kongruenz (54) genau soviel Wurzeln, als die Anzahl dieser Kombinationen von Wurzeln der Kongruenzen (55) beträgt. Somit findet sich

$$\chi(n) = \chi(2^k) \cdot \chi(p^a) \cdot \chi(q^b) \cdots \tag{57}$$

und hieraus mit Rücksicht auf die voraufgeschickten einfacheren Fälle das allgemeinere Resultat:

Ist π die Anzahl der verschiedenen ungeraden Primfaktoren, welche in n aufgehen, so ist die Anzahl der Wurzeln der Kongruenz (54)

$$\begin{aligned} \chi(n) &= 2^{\pi}, && \text{wenn } k = 0 \text{ oder } 1, \\ \chi(n) &= 2^{\pi+1}, && \text{wenn } k = 2, \\ \chi(n) &= 2^{\pi+2}, && \text{wenn } k > 2. \end{aligned} \tag{58}$$

9. Dies vorausgeschickt, sei nun $r_1, r_2, \ldots r_\nu$, wo $\nu = \varphi(n)$, irgend ein reduziertes Restsystem (mod. n). Bezeichnet r ein beliebiges Glied desselben, so hat die Kongruenz

$$rx \equiv 1 \pmod{n}$$

eine, aber auch nur eine Wurzel, bestimmt also eindeutig eine, ebenfalls dem reduzierten Restsysteme angehörige Zahl s derart, dafs

$$rs \equiv 1 \pmod{n}$$

wird. Diese Zahl s kann nur dann gleich r sein, wenn r eine Wurzel der Kongruenz (54) ist; scheidet man demnach die $\chi(n)$ Wurzeln der letzteren, die offenbar sämtlich zu n prim sind, aus dem reduzierten Restsysteme aus, so lassen sich die übrigen Glieder desselben paarweise zusammenfassen in der Weise, dafs das Produkt eines jeden Paares kongruent 1 (mod. n) wird. Mithin ist $\varphi(n) - \chi(n)$ eine gerade Zahl, welche 2δ heifse, und es resultiert eine Reihe von δ Kongruenzen, wie folgt:

(59) $$\left.\begin{array}{r} r_1 s_1 \equiv 1 \\ r_2 s_2 \equiv 1 \\ \cdot\ \cdot\ \cdot \\ r_\delta s_\delta \equiv 1 \end{array}\right\} \pmod{n}.$$

Ist andererseits r eine Wurzel der Kongruenz (54), so ist auch $x \equiv -r$ eine und zwar von der erstern verschiedene Wurzel derselben; in der That sind die Wurzeln der Kongruenzen (55) paarweise einander entgegengesetzt*), und den beiden Wurzelkombinationen

$$\lambda, \quad \alpha, \quad \beta, \ldots,$$
$$-\lambda, -\alpha, -\beta, \ldots$$

entsprechen zwei, (mod. n) entgegengesetzte, verschiedene Wurzeln der Kongruenz (54), den einzigen Fall ausgenommen, wo $\pi = 0$, $k = 1$ also $n = 2$ ist, von welchem wir absehen dürfen. Ordnet man hiernach die, aus dem reduzierten Restsysteme vorher ausgesonderten Wurzeln dieser Kongruenz auch paarweise zusammen, so wie sie (mod. n) entgegengesetzt sind, also ein Produkt $\equiv -1$ ergeben:

$$r(-r) \equiv -r^2 \equiv -1 \pmod{n},$$

so stellt sich dem Systeme (59) von Kongruenzen ein anderes von $\varepsilon = \frac{1}{2}\chi(n)$ Kongruenzen:

(60) $$\left.\begin{array}{r} r' s' \equiv -1 \\ r'' s'' \equiv -1 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ r^{(\varepsilon)} s^{(\varepsilon)} \equiv -1 \end{array}\right\} \pmod{n}$$

an die Seite, derart, dafs die sämtlichen Zahlen $r_1, s_1, \ldots r_\delta, s_\delta$, $r', s', \ldots r^{(\varepsilon)}, s^{(\varepsilon)}$ das gesamte reduzierte Restsystem (mod. n) ausmachen; ihr Produkt wird mithin dem Produkte $r_1 \cdot r_2 \ldots r_\nu$ aller Glieder des letzteren kongruent sein. Durch Multiplikation der Kongruenzen (59), (60) in einander gelangt man daher zu der Beziehung:

(61) $$r_1 r_2 \ldots r_\nu \equiv (-1)^{\frac{1}{2}\chi(n)} \pmod{n},$$

welche den verallgemeinerten **Wilson**schen Satz zum Ausdrucke bringt. In der That ist, da von dem Falle $n = 2$ abgesehen

---

*) Dies trifft zwar für $k = 1$ d. i. für die Kongruenz $x^2 \equiv 1$ (mod. 2) nicht zu, doch kann in diesem Falle die Kombination

$$1, \ -\alpha, \ -\beta, \ldots$$

auch durch

$$-1, \ -\alpha, \ -\beta, \ldots$$

ersetzt werden, welche der anderen:

$$1, \ \alpha, \ \beta, \ldots$$

durchweg entgegengesetzt ist.

wird, nach den zuvor angegebenen Werten von $\chi(n)$ der Exponent $\frac{1}{2}\chi(n)$ ungerade nur in den Fällen $k = 0, 1$; $\pi = 1$ oder $k = 2$, $\pi = 0$ d. h. in den Fällen $n = p^a$, $2p^a$ oder 4; in allen übrigen Fällen ist er gerade; dies stimmt aber völlig mit der Aussage des verallgemeinerten Wilsonschen Satzes überein.

Auf eine andere, der schon erwähnten Gaufsschen Herleitung des einfachen analoge Begründung des verallgemeinerten Wilsonschen Satzes mittels der Theorie der binomischen Kongruenzen, welche Arndt (*Journ. f. Math.* 31, 1846, p. 329) gegeben hat, kommen wir im Kap. 7, Nr. 7 zurück.

10. Anknüpfend an seine Verallgemeinerung der Eulerschen Funktion $\varphi(n)$ (Kap. 3, Nr. 11) hat Schemmel einen Satz mitgeteilt, welcher den Wilsonschen Lehrsatz als einen besonderen Fall in sich enthält, und L. Goldschmidt hat ihn zugleich mit den übrigen Schemmelschen Sätzen bewiesen. Hier sei nur ein interessanter Spezialfall jenes Schemmelschen Satzes hervorgehoben, um eine einfache direkte Herleitung dafür zu geben; dieser besondere Satz lautet: Das Produkt derjenigen zu n primen Zahlen $< n$, welche, um 1 vergröfsert, wieder prim gegen n sind, ist kongruent 1 (mod. n).

Es mag zuerst bemerkt werden, dafs der Modulus n hierbei als ungerade zu betrachten ist, denn für einen geraden Modulus n giebt es Zahlen, wie der Satz sie voraussetzt, überhaupt nicht, da eine zu ihm prime Zahl ungerade, um 1 vermehrt also gerade d. i. nicht zu n prim sein würde.

Ferner leuchtet der Satz für einen Primzahlpotenz-Modulus $n = p^a$ unmittelbar ein, denn von sämtlichen zu p^a primen Resten:

$$1, 2, 3, \ldots p-1;\ p+1,\ p+2, \ldots 2p-1; \ldots$$
$$\ldots (p^{a-1}-1)p+1,\ (p^{a-1}-1)p+2, \ldots (p^{a-1}-1)p+p-1,$$

deren Produkt nach dem verallgemeinerten Wilsonschen Satze kongruent -1 (mod. p^a) ist, gehören nur die Reste

$$(62) \qquad 1\cdot p-1,\ 2p-1,\ 3p-1, \ldots p^{a-1}\cdot p-1$$

nicht zu den Zahlen, von denen der Satz spricht, und demnach mufs das Produkt der letztern kongruent $+1$ sein (mod. p^a), wenn sich nachweisen läfst, dafs dasjenige der Zahlen (62) kongruent -1 ist. Hierzu bemerke man, dafs der socius jeder dieser Zahlen, welche die gemeinsame Form $zp-1$ haben, also diejenige Zahl x, für welche $(zp-1)x \equiv 1$ (mod. p^a) ist, offenbar dieselbe Form haben, also der Reihe (62) selbst angehörig sein mufs. Ferner ist aber eine solche Zahl $zp-1$ dann und nur dann sich selbst associiert, also $(zp-1)^2 \equiv 1$ (mod. p^a), wenn z durch p^{a-1} teilbar ist, was nur bei der letzten

Zahl der Reihe (62) zutrifft. Also mufs das ganze Produkt der Zahlen (62) dieser letzten von ihnen (mod. p^{α}) kongruent also auch $\equiv -1$ (mod. p^{α}) sein, w. z. b. w.

Ist nun $abc\ldots$ das Produkt mehrerer zu je zweien teilerfremder ungerader Zahlen, so giebt nach Kap. 3 Nr. 8 und 9 die Kongruenz

$$(63)\qquad \varrho \equiv \alpha r + \beta s + \gamma t + \cdots \pmod{n},$$

in welcher $r, s, t, \ldots$ den Bedingungen genügen, dafs

$$r \equiv 1 \pmod{a}, \quad r \equiv 0 \left(\text{mod.}\ \frac{n}{a}\right)$$

$$s \equiv 1 \pmod{b}, \quad s \equiv 0 \left(\text{mod.}\ \frac{n}{b}\right)$$

$$t \equiv 1 \pmod{c}, \quad t \equiv 0 \left(\text{mod.}\ \frac{n}{c}\right)$$

$$\cdots\cdots\cdots\cdots\cdots$$

sei, sämtliche Reste (mod. n), wenn man für $\alpha, \beta, \gamma, \ldots$ sämtliche Reste (mod. $a, b, c, \ldots$) resp. setzt, und zugleich wird ϱ dann aber auch nur dann prim gegen n, wenn $\alpha, \beta, \gamma, \ldots$ prim sind resp. gegen die letzteren Moduln. Insbesondere wird

$$1 \equiv 1 \cdot r + 1 \cdot s + 1 \cdot t + \cdots$$

also auch

$$\varrho + 1 \equiv (\alpha + 1) r + (\beta + 1) s + (\gamma + 1) t + \cdots \pmod{n}$$

und $\varrho + 1$ dann und nur dann prim gegen n sein, wenn $\alpha + 1$, $\beta + 1$, $\gamma + 1, \cdots$ es sind gegen $a, b, c, \ldots$ resp. Hiernach wird ϱ dann und nur dann einer der Reste (mod. n) sein, wie sie in dem Schemmelschen Satze vorausgesetzt werden, wenn gleichzeitig $\alpha, \beta, \gamma, \ldots$ derartige Reste (mod. a), (mod. b), (mod. c), ... resp. sind. Daher findet man aus (63) das auf die sämtlichen bezeichneten Reste ϱ (mod. n) ausgedehnte Produkt

$$(64)\qquad \begin{aligned} \Pi\varrho &\equiv (\Pi\alpha)^{\mathfrak{b}\mathfrak{c}\cdots} \pmod{a} \\ \Pi\varrho &\equiv (\Pi\beta)^{\mathfrak{a}\mathfrak{c}\cdots} \pmod{b} \\ \Pi\varrho &\equiv (\Pi\gamma)^{\mathfrak{a}\mathfrak{b}\cdots} \pmod{c} \\ &\cdots\cdots\cdots, \end{aligned}$$

wo $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ die Anzahl der bezeichneten Reste $\alpha, \beta, \gamma, \ldots$ und $\Pi\alpha, \Pi\beta, \Pi\gamma, \ldots$ die auf sie ausgedehnten Produkte bedeuten. Werden also $a, b, c, \ldots$ als die Primzahlpotenzen angesehen, aus denen sich n zusammensetzt, so werden die letztbezeichneten Produkte zufolgedessen, was voraufbemerkt worden ist, nach (64) also auch $\Pi\varrho$ in Bezug auf die Moduln $a, b, c, \ldots$ kongruent 1, und da diese zu je zweien teilerfremd sind, auch

$$\Pi\varrho \equiv 1 \pmod{n},$$

w. z. b. w.

11. Wir fügen noch einen Steinerschen Satz an (*Journ. f. Math.* 13, 1835, p. 356), der gleichfalls den Wilsonschen, wenn auch nur als einen Folgesatz, umschliefst. Die Methode, deren sich Steiner zur Herleitung seines Satzes bedient, beruht, wie die Lagrangesche Herleitung des Fermatschen Satzes, den sie voraussetzt, auf einer algebraischen Identität. Sind nämlich $r_1, r_2, \ldots r_{p-1}$ die Glieder irgend eines reduzierten Restsystems für den Primzahlmodulus p, so ist identisch

$$x = (x - r_1) + r_1;$$

wird diese Gleichheit beiderseits mit $x - r_2$ multipliziert, so giebt eine leichte Umformung die neue Identität

$$x^2 = (x - r_1)(x - r_2) + (r_1 + r_2)(x - r_1) + r_1^2,$$

deren Multiplikation mit $x - r_3$ zur folgenden führt:

$$x^3 = (x - r_1)(x - r_2)(x - r_3) + (r_1 + r_2 + r_3)(x - r_1)(x - r_2) \\ + (r_1^2 + r_1 r_2 + r_2^2)(x - r_1) + r_1^3,$$

u. s. w., bis man endlich auf die nachstehende kommt:

$$\begin{aligned} x^{p-1} = & (x - r_1)(x - r_2)(x - r_3) \cdots (x - r_{p-1}) \\ & + (r_1 + r_2 + \cdots r_{p-1}) \cdot (x - r_1)(x - r_2) \cdots (x - r_{p-2}) \\ & + (r_1^2 + r_1 r_2 + r_1 r_3 + \cdots + r_{p-2}^2) \cdot (x - r_1) \cdots (x - r_{p-3}) \\ & \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ & + (r_1^{p-2} + r_1^{p-3} r_2 + \cdots + r_2^{p-2}) \cdot (x - r_1) \\ & + r_1^{p-1} \end{aligned}$$

oder, wenn

$$X_n = (x - r_1)(x - r_2) \cdots (x - r_n)$$

gesetzt, und unter A_n die Summe der Kombinationen aus je n der Zahlen $r_1, r_2, \ldots r_{p-n}$ mit Wiederholungen aber ohne Versetzungen verstanden wird,

$$(65) \quad x^{p-1} = X_{p-1} + A_1 X_{p-2} + A_2 X_{p-3} + \cdots + A_{p-2} X_1 + A_{p-1}.$$

Hierin ist speziell $A_{p-1} = r_1^{p-1}$. Setzt man nun in dieser Identität für x irgend eine durch p nicht teilbare ganze Zahl, so folgt, da nach dem Fermatschen Satze x^{p-1}, r_1^{p-1} den gleichen Rest (mod. p) lassen, für jede solche Zahl x aus (65) die Kongruenz

$$(66) \quad X_{p-1} + A_1 X_{p-2} + \cdots + A_{p-3} X_2 + A_{p-2} X_1 \equiv 0 \pmod{p}.$$

Wird mithin jetzt für x ein von r_1 verschiedener Rest vorausgesetzt, so mufs x mit einer der übrigen Zahlen $r_2, r_3, \ldots r_{p-1}$ z. B. mit r_2 kongruent sein; für einen solchen Wert von x geben daher die Funktionen $X_{p-1}, X_{p-2}, \ldots X_2$ den Rest Null, während X_1 (mod. p) davon verschieden ist, und man schliefst also aus (66) $A_{p-2} \equiv 0$. Infolge davon besteht für jedes zu p prime x die einfachere Kongruenz

$$X_{p-1} + A_1 X_{p-2} + \cdots + A_{p-3} X_2 \equiv 0;$$

indem man den Rest von x von r_1, r_2 verschieden, etwa kongruent r_3 wählt, erschliefst man aus ihr $A_{p-3} \equiv 0$, u. s. w., bis endlich auch $A_1 \equiv 0$ gefunden wird. Somit ergiebt sich folgender Lehrsatz:

Sind $r_1, r_2, \ldots r_n$ mehrere beliebige, zur Primzahl p teilerfremde und nach ihr inkongruente Zahlen, so ist die Summe der Kombinationen zu je $p-n$ dieser Zahlen mit Wiederholungen aber ohne Versetzungen teilbar durch p.

Auf analytischem Wege hat Jacobi (*Journ. f. Math.* 14, 1835, p. 64) diesem Satze noch eine weitere Ausdehnung gegeben, und einen noch umfassenderen Satz findet man in den Anmerkungen zu den neuestens erschienenen *Vorlesungen über Zahlentheorie* von Kronecker, herausg. von K. Hensel, I, 1901, p. 504; s. ferner K. Hensel, *Archiv d. Math. u. Phys.* (3) 1, 1901, p. 319.

Dem Steinerschen Satze zufolge nimmt die Identität (65), als Kongruenz betrachtet, die folgende Gestalt an:

$$(67) \qquad x^{p-1} - 1 \equiv (x - r_1)(x - r_2) \cdots (x - r_{p-1}) \pmod{p}.$$

Das ist aber genau diejenige Kongruenz, deren sich Lagrange zur Herleitung des Fermatschen Satzes bedient hat. Setzt man in ihr $x \equiv 0$, so entsteht der Wilsonsche Lehrsatz

$$r_1 r_2 \ldots r_{p-1} \equiv -1 \pmod{p},$$

den wir daher zugleich mit der Kongruenz (67) auf neuem Wege bewiesen haben.

12. Zum Abschlusse der Betrachtung des Wilsonschen Satzes seien einige Bemerkungen mitgeteilt, denen ein mehr oder weniger grofses Interesse innewohnt.

Ihm zufolge ist die Summe

$$1 \cdot 2 \cdot 3 \cdots (p-1) + 1$$

durch die Primzahl p, möglicherweise sogar durch eine höhere Potenz von p teilbar, aber es läfst sich nach Liouville (*Journ. de Math.* (2) 1, 1856, p. 351) zeigen, dafs die Summe keine Potenz von p selbst, nämlich nicht

$$(68) \qquad 1 \cdot 2 \cdot 3 \cdots (p-1) + 1 = p^k$$

sein kann, sobald $p > 5$; für $p = 2, 3$ dagegen findet die Gleichung statt, wenn $k = 1$, für $p = 5$, wenn $k = 2$ gewählt wird. Fände sie aber sonst statt, so hätte man

$$1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) = p^k - 1$$

folglich

$$1 \cdot 2 \cdot 3 \cdots (p-2) = p^{k-1} + p^{k-2} + \cdots + p + 1.$$

Da $p > 5$ vorausgesetzt wird, finden sich unter den Faktoren des Produkts zur Linken die voneinander verschiedenen Faktoren 2 und $\frac{p-1}{2}$, deren Produkt $p-1$ demnach auch die rechte Seite teilen

müfste, während diese (mod. $p-1$) mit k kongruent ist. Folglich müfste k durch $p-1$ teilbar und also mindestens gleich $p-1$ sein; dann würde aber $1 \cdot 2 \cdot 3 \cdots (p-1)$ nach (68) mindestens gleich $p^{p-1}-1$, während es doch kleiner als $(p-1)^{p-1}$ d. i. $< p^{p-1}-1$ ist.

Ganz dasselbe schliefst man unter der gleichen Annahme $p > 5$ für die Gleichung

$$\left(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\right)^2 + 1 = p^k; \tag{69}$$

denn, schreibt man diese in der Gestalt:

$$1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \cdot 1 \cdot 3 \cdot 4 \cdots \frac{p-3}{2} = \frac{p^k-1}{p-1},$$

so erschliefst man wieder ebenso, dafs k durch $p-1$ teilbar, folglich

$$\left(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\right)^2 \gtreqq p^{p-1}-1$$

sein müfste, obwohl es doch $< \left(\frac{p-1}{2}\right)^{p-1}$ d. i. $< p^{p-1}-1$ ist. Für $p=5$ dagegen besteht die Gleichung (69), wenn man $k=1$ setzt. —

Wenn man im Wilsonschen Satze

$$1 \cdot 2 \cdot 3 \cdots (p-1) \equiv -1 \pmod{p}$$

je zwei Faktoren h, $p-h$ zusammenfafst, deren Produkt $\equiv -h^2$ ist, so nimmt er die andere Gestalt an:

$$\left(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

Da im Falle $p = 4z+3$ die rechte Seite dieser Kongruenz die positive Einheit ist, schliefst man sogleich, dafs in diesem Falle

$$1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \equiv \pm 1 \pmod{p} \tag{70}$$

ist. Hierauf hat schon Lagrange gelegentlich seines Beweises des Wilsonschen Satzes aufmerksam gemacht, aber Lejeune Dirichlet hat zuerst (*Journ. f. Math.* 3, 1828, p. 407) die Frage gestellt, wie es zu entscheiden sei, ob das obere oder das untere Vorzeichen gelte. Da $+1$ stets ein sogenannter „quadratischer Rest" von p (s. folgendes Kap.), dagegen -1 für Primzahlen der vorausgesetzten Form stets ein „quadratischer Nichtrest" und ferner (s. daselbst Nr. 2) das Produkt mehrerer Zahlen quadratischer Rest oder Nichtrest ist, jenachdem unter ihnen sich eine gerade oder ungerade Anzahl quadratischer Nichtreste befindet, so läfst sich die Frage leicht dahin beantworten, dafs in (70) das positive oder das negative Vorzeichen genommen werden müsse, jenachdem die Anzahl β der quadratischen Nichtreste von p, welche $< \frac{p}{2}$ sind, gerade oder ungerade ist, in Zeichen:

$$1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \equiv (-1)^{\beta} \pmod{p}. \tag{71}$$

Wie nun aber diese Beschaffenheit von β festzustellen sei, dafür sind verschiedene Regeln gegeben worden, welche ihren Ausgang davon nehmen, dafs zwischen der gedachten Anzahl und der Theorie „der quadratischen Formen", insbesondere der Anzahl der sogenannten „Klassen solcher Formen" ein inniger Zusammenhang besteht. Hier kann auf diese Regeln nur hingewiesen werden; s. darüber Jacobi (*Journ. f. Math.* 9, 1832, p. 189), Liouville sowie Kronecker (*Journ. de Math.* (2) 5, 1860, p. 127 und 267).

Endlich machen wir noch eine Anwendung des Wilsonschen Satzes zur Ergänzung einer früheren Untersuchung (Kap. 2, Nr. 11). Dort haben wir die höchste Potenz einer Primzahl p bestimmt, die im Produkte $1 \cdot 2 \cdot 3 \cdots n$ als Faktor enthalten ist; ist sie p^ν, so ist $\frac{n!}{p^\nu}$ eine zu p prime ganze Zahl; man kann nach dem Reste fragen, den sie (mod. p) läfst. Wenn aber

$$n = pn' + r, \quad n' = pn'' + r', \quad n'' = pn''' + r'', \cdots$$

gesetzt wird, wobei $r, r', r'' \cdots < p$ sind, so war

$$\nu = n' + n'' + n''' + \cdots.$$

Die durch p teilbaren Faktoren des Produktes $n!$ sind $p, 2p, 3p, \ldots n'p$, ihr Produkt ist

$$1 \cdot 2 \cdot 3 \cdots n'! p^{n'},$$

und, setzt man

$$n! = n'! p^{n'} \cdot R, \tag{72}$$

d. h. nennt man R das Produkt der übrigen Faktoren, so findet sich letzteres mit

$$[1 \cdot 2 \cdot 3 \cdots (p-1)]^{n'} \cdot 1 \cdot 2 \cdot 3 \cdots r$$

(mod. p) kongruent, also nach dem Wilsonschen Lehrsatze

$$R \equiv (-1)^{n'} \cdot r! \pmod{p}. \tag{72^a}$$

Ebenso aber ist

$$n'! = n''! p^{n''} \cdot R' \tag{73}$$

$$R' \equiv (-1)^{n''} \cdot r'! \pmod{p} \tag{73^a}$$

$$n''! = n'''! p^{n'''} \cdot R'' \tag{74}$$

$$R'' \equiv (-1)^{n'''} \cdot r''! \pmod{p} \tag{74^a}$$

. . . .

und durch Multiplikation der Gleichungen (72), (73), (74), ... ergiebt sich unter Berücksichtigung der Kongruenzen (72^a), (73^a), (74^a), ... die Kongruenz

$$\frac{n!}{p^\nu} \equiv (-1)^\nu \cdot r!\, r'!\, r''! \cdots \pmod{p}$$

d. h. der gesuchte Rest von $\frac{n!}{p^\nu}$ (mod. p). (L. Stickelberger, *Math. Ann.* 37, 1890, p. 321; K. Hensel, *Arch. d. Math. u. Phys.* (3), 2, p. 294.)

Sechstes Kapitel.

Die Theorie der quadratischen Reste.

1. Mit dem Fermatschen Satze sind wir über die Kongruenzen ersten Grades hinaus zu solchen höheren Grades übergegangen und haben dann in der Folge für die Kongruenz zweiten Grades $x^2 \equiv 1 \pmod{n}$ die Anzahl ihrer Wurzeln bestimmt. Betrachten wir nun allgemein die Kongruenzen zweiten Grades, die in systematischer Folge denen des ersten Grades zunächst stehen! Ihre allgemeine Form ist

$$(1) \qquad ax^2 + bx + c \equiv 0 \pmod{m},$$

wo a, b, c ganze Zahlen bedeuten, deren erstere durch m nicht aufgeht. Diese Kongruenz ist ersichtlich völlig gleichbedeutend mit der anderen:

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{4am},$$

welcher man die Form geben kann:

$$(2) \qquad (2ax + b)^2 \equiv b^2 - 4ac \pmod{4am}.$$

Indem man

$$(3) \qquad 2ax + b \equiv z \pmod{4am}$$

setzt, kommt man auf die einfachere quadratische Kongruenz

$$(4) \qquad z^2 \equiv b^2 - 4ac \pmod{4am}$$

zurück, welche demnach auflösbar sein mufs, wenn die gegebene Kongruenz (1) es sein soll. Gesetzt, sie sei auflösbar, so würde man für jede Lösung z derselben versuchen müssen, ob die Kongruenz (3) auflösbar, ob nämlich $z - b$ durch den gröfsten gemeinsamen Teiler $2a$ des Koeffizienten von x und des Modulus teilbar sei; ist dies der Fall, so giebt es, und nur in diesem Falle, eine entsprechende Zahl x, welche die Kongruenz (1) erfüllt.

Hiernach dürfen wir hinfort unsere Betrachtung auf die quadratischen Kongruenzen der einfacheren Gestalt:

$$(5) \qquad x^2 \equiv m \pmod{n},$$

in welcher m, n beliebige ganze Zahlen sind, beschränken. Dabei darf der Modulus n positiv gedacht werden. Wir setzen zunächst m, n als relativ prime Zahlen voraus. Jenachdem dann diese Kongruenz auflösbar ist oder nicht, heifst m quadratischer Rest oder Nichtrest (Rest oder nicht Rest einer Quadratzahl) (mod. n). Nehmen wir an, das erstere sei der Fall und $x = \xi$ eine Lösung von (5), so dafs

$$\xi^2 \equiv m \pmod{n}$$

ist. Ist dann z irgend eine Lösung der Kongruenz

(6) $$z^2 \equiv 1 \pmod{n},$$

so leuchtet ein, dafs auch $x \equiv \xi z$ eine Lösung von (5), nämlich $(\xi z)^2 \equiv m \pmod{n}$ ist. Umgekehrt, wenn ξ' noch eine zweite Lösung von (5) ist, mithin $\xi'^2 \equiv m$ also auch $\xi'^2 \equiv \xi^2 \pmod{n}$ ist, so sei η der socius von $\xi \pmod{n}$ — ein solcher ist vorhanden, da ξ nach der Annahme über m prim gegen n ist — es sei also $\xi\eta \equiv 1 \pmod{n}$. Alsdann findet sich $(\xi'\eta)^2 \equiv (\xi\eta)^2 \equiv 1$, $\xi'\eta$ ist also eine Lösung z der Kongruenz (6) und demnach $\xi' \equiv \xi z \pmod{n}$.

Aus dieser Betrachtung geht hervor, dafs man aus einer Lösung der Kongruenz (5) ihre sämtlichen Lösungen erhält, wenn man jene mit den Lösungen der Kongruenz (6) multipliziert; und da für zwei solche Lösungen z, z' die Produkte $\xi z, \xi z' \pmod{n}$ kongruent oder nicht kongruent sind, jenachdem z, z' es sind, so ist die Anzahl der Wurzeln der Kongruenz (5), falls sie deren überhaupt hat d. i. auflösbar ist, gleich der Anzahl $\chi(n)$ der Wurzeln der Kongruenz (6).

Es fragt sich also nun, unter welchen Bedingungen die Kongruenz (5) auflösbar ist. Sei allgemein

$$n = 2^k p^a q^b \ldots,$$

dann leuchtet zunächst ein, dafs für die Möglichkeit der Kongruenz (5) diejenige der Kongruenzen

(7) $$x^2 \equiv m \pmod{2^k}, \quad x^2 \equiv m \pmod{p^a}, \quad x^2 \equiv m \pmod{q^b}, \ldots$$

notwendig und hinreichend ist (die erste derselben fällt fort, sobald $k = 0$ d. i. n durch 2 nicht teilbar ist). Denn einerseits folgen diese aus jener; aber auch umgekehrt: sind sie möglich und $\eta, \xi, \xi', \ldots$ je eine Lösung der ersten, zweiten, dritten u. s. f., sodafs

$$\eta^2 \equiv m \pmod{2^k}, \quad \xi^2 \equiv m \pmod{p^a}, \quad \xi'^2 \equiv m \pmod{q^b}, \ldots,$$

so giebt es eine Zahl x, welche den Kongruenzen

$$x \equiv \eta \pmod{2^k}, \quad x \equiv \xi \pmod{p^a}, \quad x \equiv \xi' \pmod{q^b}, \ldots$$

und demnach jeder der Kongruenzen (7) genügt; daher erfüllt diese Zahl auch die Kongruenz (5).

Nun ist zunächst, wenn $k = 1$ ist, die Kongruenz

(8) $$x^2 \equiv m \pmod{2^k},$$

in welcher nach der Annahme, dafs m und der Modulus teilerfremd seien, m ungerade ist, immer auflösbar, nämlich durch jede ungerade Zahl erfüllt.

Ist $k = 2$, die Kongruenz also diese:

$$x^2 \equiv m \pmod{4},$$

so kann jede ihrer Lösungen nur eine ungerade Zahl $2z + 1$ sein, deren Quadrat $4z^2 + 4z + 1 \equiv 1 \pmod{4}$ ist; demnach erfordert

die Kongruenz (8) in diesem Falle, dafs $m \equiv 1 \pmod{4}$ sei, ist dann aber auch möglich, nämlich durch jede ungerade Zahl x erfüllt.

Ist $k \geqq 3$, soll mithin auch

$$x^2 \equiv m \pmod{8}$$

sein, so mufs wieder x eine ungerade Zahl d. i. von der Form $4z \pm 1$ sein, deren Quadrat $16z^2 \pm 8z + 1 \equiv 1 \pmod{8}$ ist; somit erfordert in diesem Falle die Kongruenz (8), dafs $m \equiv 1 \pmod{8}$ sei, ist dann aber auch möglich. Dies leuchtet ein, falls $k = 3$, die Kongruenz also diese:

$$x^2 \equiv m \pmod{8}$$

ist, denn die letztere wird, wenn $m \equiv 1 \pmod{8}$ ist, durch jede ungerade Zahl erfüllt. Gesetzt aber, dasselbe sei schon für die Kongruenz

$$x^2 \equiv m \pmod{2^{k-1}}$$

erwiesen, wo nun $k - 1 \geqq 3$, und ξ sei eine Lösung derselben, sodafs

$$\xi^2 - m = 2^{k-1} \cdot h$$

ist, so würde, wenn man z durch die Kongruenz

$$h + \xi z \equiv 0 \pmod{2}$$

bestimmt,

$$(\xi + 2^{k-2} \cdot z)^2 \equiv m + 2^{k-1}(h + \xi z) \equiv m \pmod{2^k}$$

also auch die Kongruenz (8) erfüllt. Hierdurch ist die Behauptung als allgemein giltig erwiesen.

Soll ferner eine Kongruenz von der Form

$$(9) \qquad x^2 \equiv m \pmod{p^a}$$

möglich sein, so mufs sie offenbar auch für jede niedrigere Potenz von p als Modulus, zuletzt also auch die Kongruenz

$$(10) \qquad x^2 \equiv m \pmod{p}$$

möglich d. h. m quadratischer Rest von p sein. Diese notwendige Bedingung ist aber auch hinreichend. Denn, sobald die Kongruenz

$$x^2 \equiv m \pmod{p^{a-1}},$$

wo $a - 1 \geqq 1$, eine Lösung $x = \xi$ hat, sodafs $\xi^2 - m = p^{a-1} \cdot h$, so ergiebt sich, wenn z durch die Kongruenz $h + 2\xi z \equiv 0 \pmod{p}$ bestimmt wird,

$$(\xi + p^{a-1} \cdot z)^2 \equiv m + p^{a-1}(h + 2\xi z) \equiv m \pmod{p^a}$$

also ist auch die Kongruenz

$$x^2 \equiv m \pmod{p^a}$$

auflösbar; ist mithin m quadratischer Rest von p, d. h. die Kongruenz (10) auflösbar, so ist sie es auch $(\text{mod. } p^2)$, dann auch $(\text{mod. } p^3), \ldots$ endlich auch $(\text{mod. } p^a)$.

Diese Resultate, verbunden mit dem, was über die eventuelle Anzahl der Wurzeln ausgesagt worden ist, lassen sich zusammenfassen in folgenden Satz:

Zur Möglichkeit der Kongruenz

$$(5) \qquad x^2 \equiv m \pmod{n = 2^k p^a q^b \cdots},$$

in welcher m prim ist gegen n, ist notwendig und hinreichend,

1) wenn $k = 0$ oder 1 ist, dafs m quadratischer Rest sei von jeder der Primzahlen $p, q, \ldots$;

2) wenn $k = 2$ ist, dafs aufserdem $m \equiv 1 \pmod{4}$ sei;

3) wenn $k \gtreqless 3$ ist, dafs aufserdem noch genauer $m \equiv 1 \pmod{8}$ sei.

Sind diese bezüglichen Bedingungen erfüllt, so hat die Kongruenz (5) $\chi(n)$ Wurzeln, wo $\chi(n)$ dieselbe Bedeutung hat, wie im vorigen Kapitel.

Auf den bisher betrachteten Fall, in welchem m, n relativ prime Zahlen waren, läfst sich der andere zurückführen, wo sie einen gröfsten gemeinsamen Teiler d haben. Setzt man dann nämlich $m = m'd$, $n = n'd$ und nennt jede in d enthaltene Primzahl p, so kann man die höchste in d aufgehende Potenz der letzteren mit $p^{2k+\delta}$ bezeichnen, indem man $\delta = 0$ oder 1 setzt, jenachdem die Potenz eine gerade oder eine ungerade ist; demnach wollen wir

$$d = \Pi(p^{2k+\delta})$$

schreiben. Soll nun die Kongruenz

$$(11) \qquad x^2 \equiv m \pmod{n}$$

lösbar sein, so mufs auch x^2 durch d und folglich x durch jede der Potenzen $p^{k+\delta}$ teilbar sein; wir setzen mithin

$$x = \Pi(p^{k+\delta}) \cdot y$$

und erhalten aus (11) die äquivalente Kongruenz

$$(12) \qquad \Pi(p^\delta) \cdot y^2 \equiv m' \pmod{n'},$$

in welcher m', n' relativ prime Zahlen sind. Deshalb dürfen auch $\Pi(p^\delta)$ und n' keinen Teiler gemein haben, was also eine erste Bedingung für die Möglichkeit der Kongruenz (11) ausmacht. Aus (12) aber folgt, indem man

$$z = \Pi(p^\delta) \cdot y$$

setzt,

$$(13) \qquad z^2 \equiv \Pi(p^\delta) \cdot m' \pmod{n'}$$

und es mufs daher zweitens $\Pi(p^\delta) \cdot m'$ quadratischer Rest von n' sein, damit (11) auflösbar sei. Sind aber diese beiden Bedingungen erfüllt, so hat die vorstehende Kongruenz eine Lösung z und zugleich giebt es eine Zahl P derart, dafs $P \cdot \Pi(p^\delta) \equiv 1 \pmod{n'}$

ist; indem man die Kongruenz (13) mit P^2 multipliziert und $Pz \equiv y$ setzt, geht sie über in die Gestalt

$$y^2 \equiv Pm' \pmod{n'},$$

aus der sich sogleich die Form (12) d. h. eine Lösung der Kongruenz (11) ergiebt. Die vorher gegebenen zwei notwendigen Bedingungen reichen also zur Möglichkeit dieser Kongruenz auch hin und die Auflösung der letzteren wird auf die der Kongruenz (13) zurückgeführt, in welcher die rechte Seite und der Modulus relativ prime Zahlen sind.

2. Nach dem Hauptsatze der vorigen Nr. kommt die Frage, ob eine Zahl m in Bezug auf einen gegebenen Modulus n quadratischer Rest oder Nichtrest sei, wesentlich auf die andere zurück, wie sie sich in dieser Hinsicht zu einer Potenz von 2, sowie zu den Primfaktoren verhalte, aus denen n zusammengesetzt ist. Da sich nun bezüglich einer Potenz von 2 dieses Verhalten sogleich aus dem Umstande, ob m von der Form $4z + 1$ bezw. von der Form $8z + 1$ ist oder nicht ist, herausstellt, so bleibt uns ferner nur zu untersuchen, ob m von einer gegebenen ungeraden Primzahl p quadratischer Rest oder Nichtrest sei.

Nun ist zunächst klar, dafs (mod. p) kongruente Zahlen m, m' stets denselben „quadratischen Charakter“ haben, nämlich gleichzeitig quadratische Reste oder gleichzeitig quadratische Nichtreste von p sind; denn, ist die Kongruenz $x^2 \equiv m \pmod{p}$ lösbar, so ist für jede Lösung x derselben auch $x^2 \equiv m' \pmod{p}$. Ferner geben Zahlen x, x', welche (mod. p) kongruent sind, auch kongruente Quadrate. Endlich müssen in der Kongruenz $x^2 \equiv m \pmod{p}$ die Zahlen m, x zugleich durch p teilbar oder zugleich gegen p prim sein. Um also alle inkongruenten zu p primen quadratischen Reste zu finden, braucht man nur die Glieder irgend eines reduzierten Restsystems (mod. p) zu quadrieren und die Reste dieser Quadrate zu bilden. Sind aber r, s zwei verschiedene solche Glieder, so findet die Kongruenz $s^2 \equiv r^2 \pmod{p}$ oder

$$(s - r)(s + r) \equiv 0 \pmod{p}$$

nur statt, wenn $s \equiv -r \equiv p - r$ ist und in diesem Falle ist in der That

$$s^2 \equiv (p - r)^2 \equiv r^2 \pmod{p}.$$

Folglich geben die $p - 1$ Glieder des reduzierten Restsystems genau $\frac{p-1}{2}$ inkongruente Quadrate, oder: für einen (ungeraden) Primzahlmodulus p giebt es $\frac{p-1}{2}$ inkongruente, durch p nicht teilbare, quadratische Reste und daher ebensoviel solche quadratische Nichtreste.

Man denke sich nun das reduzierte Restsystem und nenne die Gesamtheit der quadratischen Reste desselben a, die der Nichtreste b. Multipliziert man das Restsystem mit einer zu p primen Zahl m, so bilden die Zahlen ma, mb wieder ein reduziertes Restsystem (mod. p) und daher müssen unter ihnen wieder $\frac{p-1}{2}$ quadratische Reste und $\frac{p-1}{2}$ quadratische Nichtreste sein. Nun leuchtet ein, dafs das Produkt zweier quadratischen Reste m, m' wieder ein quadratischer Rest (mod. p) sein mufs, denn aus dem Stattfinden der Kongruenzen

$$x^2 \equiv m, \quad x'^2 \equiv m' \pmod{p}$$

fliefst auch das Stattfinden der folgenden:

$$(xx')^2 \equiv mm' \pmod{p}.$$

Ist demnach der oben gedachte Multiplikator m ein quadratischer Rest von p, so sind die $\frac{p-1}{2}$ Zahlen ma lauter und folglich die sämtlichen quadratischen Reste des neuen Restsystems, mithin die $\frac{p-1}{2}$ Zahlen mb lauter Nichtreste, also ist das Produkt aus einem quadratischen Reste und einem quadratischen Nichtreste stets ein quadratischer Nichtrest (mod. p). Wird dagegen m als quadratischer Nichtrest von p gedacht, so sind dem eben Bewiesenen zufolge die $\frac{p-1}{2}$ Zahlen ma lauter und folglich die sämtlichen Nichtreste des neuen Restsystems, mithin die $\frac{p-1}{2}$ Zahlen mb lauter quadratische Reste; also ist das Produkt zweier quadratischer Nichtreste stets ein quadratischer Rest (mod. p).

Sehr bequemen Ausdruck erhalten diese und andere Sätze über quadratische Reste, wenn man sich eines von Legendre eingeführten Symbols, des Zeichens $\left(\frac{m}{p}\right)$ bedient, welches, jenachdem m quadratischer Rest oder Nichtrest ist von p, den Wert $+1$ oder -1 bedeuten soll.

Mittels dieses Legendreschen Symbols sprechen sich die erhaltenen Sätze in den einfachen Gleichungen aus:

$$\left(\frac{m}{p}\right) = \left(\frac{m'}{p}\right), \quad \text{wenn} \quad m \equiv m' \pmod{p}, \tag{14}$$

$$\left(\frac{m}{p}\right) \cdot \left(\frac{m'}{p}\right) = \left(\frac{mm'}{p}\right), \tag{15}$$

wobei die Zähler stets als prim gegen den Nenner anzunehmen sind. Der in der zweiten Gleichung ausgesprochene Satz läfst sich sogleich auf ein Produkt von mehr als zwei Faktoren ausdehnen und dann folgendermafsen fassen: Ein Produkt von Faktoren ist quadratischer Rest oder Nichtrest von p, jenachdem die Anzahl

der Faktoren, welche quadratische Nichtreste sind, gerade oder ungerade ist.

Jacobi hat dem **Legendre**schen Symbole eine Verallgemeinerung gegeben, indem er es für den Fall definiert, dafs der Nenner eine beliebige (positive) ungerade Zahl ist. Sei nämlich P eine solche und, in seine gleichen oder verschiedenen Primfaktoren zerlegt,

$$P = pp'p'' \dots, \tag{16}$$

sei ferner m eine Zahl, welche prim gegen P also auch gegen die einzelnen Faktoren $p, p', p'', \dots$ von P ist, so definiert **Jacobi** das Symbol $\left(\frac{m}{P}\right)$ durch die Gleichung

$$\left(\frac{m}{P}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right)\cdots. \tag{17}$$

Ist nun $m \equiv m'$ (mod. P), so besteht diese Kongruenz auch bezüglich eines jeden der Moduln $p, p', p'', \dots$ und aus (14) ergiebt sich daher mit Rücksicht auf die Definitionsgleichung

$$\left(\frac{m'}{P}\right) = \left(\frac{m'}{p}\right)\left(\frac{m'}{p'}\right)\left(\frac{m'}{p''}\right)\cdots$$

die folgende Gleichung:

$$\left(\frac{m}{P}\right) = \left(\frac{m'}{P}\right), \quad \text{wenn} \quad m \equiv m' \text{ (mod. } P). \tag{18}$$

Desgleichen liefert die Formel (15), wenn auch m' prim gegen P vorausgesetzt wird,

$$\left(\frac{mm'}{P}\right) = \left(\frac{m}{P}\right)\left(\frac{m'}{P}\right). \tag{19}$$

Diesen zwei fundamentalen, den Gleichungen (14), (15) analogen Beziehungen fügt sich aber hier noch eine dritte an. Sei nämlich Q eine zweite positive ungerade Zahl und, wenn sie in ihre gleichen oder ungleichen Primfaktoren zerlegt wird,

$$Q = qq'q'' \dots, \tag{20}$$

sei ferner die Zahl m nicht nur gegen P, sondern auch gegen Q und somit auch gegen deren Produkt PQ prim, so hat man nach Jacobis Definition

$$\left(\frac{m}{Q}\right) = \left(\frac{m}{q}\right)\left(\frac{m}{q'}\right)\left(\frac{m}{q''}\right)\cdots \tag{21}$$

also

$$\left(\frac{m}{P}\right)\left(\frac{m}{Q}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right)\cdots\left(\frac{m}{q}\right)\left(\frac{m}{q'}\right)\left(\frac{m}{q''}\right)\cdots$$

d. i., da

$$PQ = pp'p'' \dots qq'q'' \dots$$

ist,

$$\left(\frac{m}{PQ}\right) = \left(\frac{m}{P}\right)\left(\frac{m}{Q}\right). \tag{22}$$

Es soll endlich auch der Fall eines negativen Nenners mitumfaſst werden durch die Festsetzung

(23) $$\left(\frac{m}{-P}\right) = \left(\frac{m}{P}\right).$$

Befolgt nun gleich das verallgemeinerte Legendresche Symbol ganz analoge Gesetze, wie das ursprüngliche, so muſs doch auch ein wesentlicher Unterschied zwischen beiden angemerkt werden. Jenachdem nämlich $\left(\frac{m}{p}\right) = +1$ oder -1 ist, ist der Definition Legendres gemäſs $x^2 \equiv m \pmod{p}$ möglich oder unmöglich. Nun ist zwar auch, falls $x^2 \equiv m \pmod{P}$ möglich ist, $\left(\frac{m}{P}\right) = +1$, da alsdann diese Kongruenz auch nach den einzelnen Primfaktoren von P als Moduln besteht, die einzelnen Faktoren des Symbols $\left(\frac{m}{P}\right)$ also sämtlich gleich $+1$ sind; umgekehrt kann aber $x^2 \equiv m \pmod{P}$ unmöglich sein, ohne daſs deshalb $\left(\frac{m}{P}\right) = -1$ wäre, oder aus $\left(\frac{m}{P}\right) = +1$ ist nicht auch umgekehrt auf die Möglichkeit jener Kongruenz zu schlieſsen; in der That wird sie unlösbar sein, sobald sie es auch nur in Bezug auf einen einzigen der Primfaktoren $p, p', p'', \ldots$ ist; gleichzeitig würde aber dennoch $\left(\frac{m}{P}\right) = +1$ sein, falls dies in Bezug auf eine gerade Anzahl der Primfaktoren der Fall, also eine gerade Anzahl Faktoren des Symbols $\left(\frac{m}{P}\right)$ gleich -1 ist.

3. Bevor wir auf Grund dieser Ergebnisse die Frage, ob eine Zahl m quadratischer Rest oder Nichtrest einer ungeraden Primzahl p sei, weiter behandeln, leiten wir ein von Euler angegebenes Kriterium*) her, welches theoretisch darüber sofort Auskunft erteilt. Es sei dabei der Modulus zunächst wieder eine beliebige Zahl n und

(24) $$r_1, r_2, r_3, \ldots r_{\varphi(n)}$$

irgend ein reduziertes Restsystem (mod. n). Ist nun m eine beliebige Zahl, die wir indessen gegen n prim annehmen wollen, so lassen, da die Kongruenz $r_i x \equiv m \pmod{n}$ stets eine Wurzel hat, sich die Reste (24), nachdem man aus ihnen diejenigen ausgesondert hat, deren Quadrate mit m kongruent sind, in eindeutiger Weise so in Paare zusammenfassen, daſs deren Glieder ein mit m kongruentes Produkt geben. Die auszuscheidenden Reste sind die Wurzeln der Kongruenz

(25) $$x^2 \equiv m \pmod{n},$$

ihre Anzahl also $\chi(n)$ oder 0, jenachdem m quadratischer Rest oder

*) Dies Kriterium findet sich ausgesprochen in Eulers Abhandlung in *Opusc. analyt.* I p. 242, 268 oder *Comm. Ar. coll.* II p. 11.

Nichtrest von n ist. Im letzteren Falle erhält man also $\frac{1}{2}\varphi(n)$ Kongruenzen von der Art:

$$(26)\qquad r_i \cdot r_k \equiv m \pmod{n},$$

wo r_i, r_k je zwei verschiedene der Reste (24) bedeuten, und wenn man sie sämtlich ineinander multipliziert, die nachstehende Beziehung:

$$(27)\qquad r_1 \cdot r_2 \cdot r_3 \cdots r_{\varphi(n)} \equiv m^{\frac{1}{2}\varphi(n)} \pmod{n}.$$

Im ersteren Falle dagegen lassen sich nur die $\varphi(n) - \chi(n)$ Glieder des Restsystems (24), welche nach Ausscheidung der Wurzeln der Kongruenz (25) überbleiben, in $\frac{1}{2}(\varphi(n) - \chi(n))$ Paare fassen, deren jedem eine Kongruenz von der Form (26) entspricht; die Wurzeln der Kongruenz (25) aber sind zu je zweien einander entgegengesetzt (mod. n) und bilden also $\frac{1}{2}\chi(n)$ der Reihe (24) angehörige Paare, deren Glieder ein Produkt

$$(26^a)\qquad r_i r_k \equiv -m \pmod{n}$$

geben; durch Multiplikation all' solcher Kongruenzen (26) und (26ª) erhält man mithin jetzt diese andere Beziehung:

$$(27^a)\qquad r_1 r_2 r_3 \ldots r_{\varphi(n)} \equiv (-1)^{\frac{1}{2}\chi(n)} \cdot m^{\frac{1}{2}\varphi(n)} \pmod{n}.$$

Dem verallgemeinerten Wilsonschen Lehrsatze zufolge ist aber

$$r_1 r_2 \ldots r_{\varphi(n)} \equiv (-1)^{\frac{1}{2}\chi(n)} \pmod{n};$$

mit Rücksicht hierauf ergeben die Kongruenzen (27) und (27ª) das folgende Resultat:

Jenachdem die Kongruenz (25) Wurzeln hat oder nicht, d. i. jenachdem m quadratischer Rest oder Nichtrest von n ist, ist

$$(28)\qquad m^{\frac{1}{2}\varphi(n)} \equiv 1 \quad \text{oder} \quad \equiv (-1)^{\frac{1}{2}\chi(n)} \pmod{n}.$$

Dieser zuerst von E. Schering (*Acta Math.* 1, 1883, p. 159) gegebene Satz ist das verallgemeinerte **Euler**sche Kriterium, welches in seiner ursprünglichen Fassung sich nur auf den Fall bezieht, wo der Modulus n eine ungerade Primzahl p ist. In diesem einfachsten Falle ist $\varphi(n) = \varphi(p) = p - 1$, $\chi(n) = 2$; demnach spricht das eigentliche **Euler**sche Kriterium den spezielleren Satz aus: dafs m quadratischer Rest oder Nichtrest einer ungeraden Primzahl p ist, jenachdem

$$(29)\qquad m^{\frac{p-1}{2}} \equiv +1 \quad \text{oder} \quad \equiv -1 \pmod{p}$$

ist. Man sieht, dafs im Grunde nur dieser spezielle Satz als Kriterium bezeichnet zu werden verdient, indem er mit Sicherheit dar-

über entscheiden lehrt, ob eine Zahl quadratischer Rest von p ist, oder nicht. Mit Anwendung des Legendreschen Symbols nimmt es die folgende Gestalt an:

$$m^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right) \pmod{p}. \tag{30}$$

Ist m' eine zweite zu p prime Zahl, so mufs in gleicher Weise

$$m'^{\frac{p-1}{2}} \equiv \left(\frac{m'}{p}\right) \pmod{p}$$

sowie auch

$$(mm')^{\frac{p-1}{2}} \equiv \left(\frac{mm'}{p}\right) \pmod{p}$$

sein, woraus sich die Kongruenz

$$\left(\frac{mm'}{p}\right) \equiv \left(\frac{m}{p}\right) \cdot \left(\frac{m'}{p}\right) \pmod{p}$$

oder, da beide Seiten den Wert $+1$ oder -1 und folglich nur dann eine durch p teilbare Differenz haben, wenn sie dieselbe Einheit darstellen, die Gleichheit

$$\left(\frac{mm'}{p}\right) = \left(\frac{m}{p}\right) \cdot \left(\frac{m'}{p}\right)$$

d. i. wieder die Formel (15) ergiebt.

Das **Euler**sche Kriterium (29) ist, wenn man den **Fermat**schen Lehrsatz benutzen will, auch folgendermafsen zu erweisen. Wenn m quadratischer Rest von p, also eine Zahl x vorhanden ist, für welche

$$x^2 \equiv m \pmod{p}$$

ist und welche, wie m selbst, prim gegen p ist, so folgt durch Erhebung zur $\frac{p-1}{2}^{\text{ten}}$ Potenz

$$x^{p-1} \equiv m^{\frac{p-1}{2}}$$

also nach dem Fermatschen Satze $m^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Hiernach hat die Kongruenz

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

die $\frac{p-1}{2}$ inkongruenten quadratischen Reste (mod. p) und, da sie nicht mehr Wurzeln haben kann, als ihr Grad beträgt, auch nur sie zu Wurzeln. Da aber für jede durch p nicht teilbare Zahl m dem Fermatschen Satze zufolge

$$m^{p-1} - 1 = \left(m^{\frac{p-1}{2}} - 1\right)\left(m^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}$$

ist, so folgt, wenn diese Zahl ein quadratischer Nichtrest ist, die Kongruenz

$$m^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Indessen kann man besser umgekehrt das unmittelbar hergeleitete **Euler**sche Kriterium zu einem neuen Beweise des **Fermat**schen Satzes benutzen. Da nämlich jenem Kriterium zufolge für jede durch p nicht teilbare Zahl m

$$\text{entweder} \quad m^{\frac{p-1}{2}} \equiv +1 \quad \text{oder} \quad m^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

ist, so wird immer, wie es der Fermatsche Satz aussagt,

$$m^{p-1} \equiv 1 \pmod{p}$$

sein.

4. Das Eulersche Kriterium oder die Kongruenz (30) ist von Gaufs durch ein anderes ersetzt worden, welches in der Wissenschaft den Namen „**Gaufs**sches Lemma" erhalten hat.

Man verstehe unter m eine durch die ungerade Primzahl p nicht teilbare ganze Zahl und bilde die Produkte

$$(31) \qquad 1 \cdot m,\ 2 \cdot m,\ 3 \cdot m,\ \cdots \frac{p-1}{2} \cdot m;$$

ihre absolut kleinsten, zwischen $\frac{p}{2}$ und $-\frac{p}{2}$ liegenden Reste (mod. p) werden teils positiv, teils negativ sein; die ersteren mögen $r_1, r_2, \ldots r_\lambda$, die anderen $-r_1', -r_2', \ldots, -r_\mu'$ heifsen. Offenbar sind je zwei r, sowie je zwei r' untereinander verschieden; aber auch jedes r wird von jedem r' verschieden sein, denn sonst müfste die Summe der ihnen entsprechenden Vielfachen (31) kongruent 0 sein, während sie doch ein Vielfaches von m wäre, kleiner als das erste durch p teilbare Vielfache pm. Die $\lambda + \mu = \frac{p-1}{2}$ Zahlen r, r' bilden demnach zusammengenommen das ganze System der Zahlen $1, 2, 3, \cdots \frac{p-1}{2}$. Daraus geht hervor, dafs

$$1 \cdot m \cdot 2m \cdot 3m \cdots \frac{p-1}{2} m \equiv (-1)^\mu r_1 r_2 \cdots r_\lambda \cdot r_1' r_2' \cdots r_\mu'$$

$$\equiv (-1)^\mu \cdot 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \pmod{p}$$

und folglich, da $1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}$ prim ist gegen p, dafs

$$(32) \qquad m^{\frac{p-1}{2}} \equiv (-1)^\mu \pmod{p}$$

oder, wenn die von den Zahlen m, p bedingte Zahl μ als eine Funktion derselben durch das Zeichen

$$(33) \qquad \mu = \mu(m, p)$$

dargestellt wird, dafs

(34) $$m^{\frac{p-1}{2}} \equiv (-1)^{\mu(m,p)} \pmod{p}$$

ist. Verbindet man diese Kongruenz mit dem Eulerschen Kriterium (30), so ergiebt sich das Gaufssche Lemma:

$$\left(\frac{m}{p}\right) = (-1)^{\mu(m,p)}$$

oder der Satz: Die Zahl m ist quadratischer Rest oder Nichtrest der ungeraden Primzahl p, jenachdem die Anzahl $\mu(m,p)$ der (mod. p) genommenen absolut kleinsten Reste der Reihe (31), welche negativ sind, gerade oder ungerade ist.

Auch dies Lemma ist wieder von Schering auf den Fall eines zusammengesetzten Modulus n ausgedehnt worden (*Berl. Monatsber.* 1876, p. 330; *Acta Math.* 1, p. 153). Kronecker (*Berl. Sitzungsber.* 1884, p. 527; vgl. dazu Bachmann, *Elem. d. Zahlenth.* 1892, p. 144 ff.) hat die Scheringschen Betrachtungen mit Verwendung seines Zeichens sgn. $R(x)$ — s. unten Nr. 10 — in einer anderen Gestalt reproduziert, von welcher die Scheringschen gewissermafsen nur eine „logarithmische Umgestaltung“ sind. Wir folgen jedoch hier bei Herleitung des verallgemeinerten Lemma's des Letztern Gange.

Für einen beliebigen ungeraden Modulus n betrachten wir die sämtlichen positiven absolut kleinsten Reste d. h. die Zahlen

(35) $$1, 2, 3, \ldots \frac{n-1}{2}.$$

Sie lassen sich in verschiedene Klassen verteilen, indem man immer diejenigen von ihnen in eine Klasse zusammenfassen kann, die mit n denselben gröfsten gemeinsamen Teiler haben. Bedeutet d jeden Teiler von n, welcher kleiner als $\frac{n}{2}$ ist, sodafs $n = dn'$, $n' > 2$ ist, und ist r eine Zahl der Reihe (35), für welche d den gröfsten mit n gemeinsamen Teiler vorstellt, so wird $r = dr'$ und $r' < \frac{n'}{2}$ und prim gegen n' sein, und umgekehrt. Sind demnach die sämtlichen positiven Zahlen, welche $< \frac{n'}{2}$ und prim gegen n' sind und deren Anzahl offenbar $\frac{1}{2}\varphi(n')$ beträgt, die Zahlen

(36) $$r_1, r_2, r_3, \ldots r_{\frac{1}{2}\varphi(n')},$$

so bilden die Zahlen

(37) $$dr_1, dr_2, dr_3, \ldots dr_{\frac{1}{2}\varphi(n')}$$

die gesamte, dem Teiler d entsprechende Klasse der Zahlen (35) und man erhält die Gesamtheit der letzteren, wenn man die Zahlen (37) für jeden der gedachten Teiler d von n aufstellt.

Dies vorausgeschickt, sei m eine gegen n und folglich auch gegen n' prime Zahl. Bildet man für sie die Produkte

$$mr_1,\ mr_2,\ \dots\ mr_{\frac{1}{2}\varphi(n')} \tag{38}$$

und deren absolut kleinste Reste (mod. n'), so erhält man $\frac{1}{2}\varphi(n')$ Kongruenzen von folgender Form:

$$mr_i \equiv \varepsilon_i r_i' \pmod{n'}, \tag{39}$$
$$\left(i = 1, 2, 3, \cdots \frac{1}{2}\varphi(n')\right)$$

wo $\varepsilon_i = \pm 1$, r_i' aber wieder eine positive Zahl $< \frac{n'}{2}$ und prim gegen n', d. h. eine der Zahlen (36) sein wird. Diese Zahlen $r_1', r_2', \dots r'_{\frac{1}{2}\varphi(n')}$ sind, wie leicht zu sehen, zu je zweien verschieden; denn, wäre $r_i' = r_k'$, so müfste

$$m(\varepsilon_k r_i - \varepsilon_i r_k) \equiv 0 \pmod{n'}$$

d. h., jenachdem die Einheiten ε_i, ε_k gleich oder entgegengesetzt sind, $r_i - r_k$ oder $r_i + r_k$ teilbar sein durch n', während doch beide Zahlen $< n'$ sind. Sonach stimmen die Zahlen $r_1', r_2', \dots r'_{\frac{1}{2}\varphi(n')}$ zusammengenommen mit den Zahlen der Reihe (36) überein, und man erschliefst aus den Kongruenzen (39), indem man sie durch Multiplikation verbindet, die folgende andere:

$$m^{\frac{1}{2}\varphi(n')} \equiv \varepsilon_1 \varepsilon_2 \dots \varepsilon_{\frac{1}{2}\varphi(n')} \pmod{n'}. \tag{40}$$

Bezeichnet man daher mit $\mu_0(m, n')$ die Anzahl derjenigen Einheiten ε_i, welche negativ sind, und beachtet das in der Kongruenz (28) ausgesprochene Scheringsche Kriterium, so findet sich zunächst der Satz:

Jenachdem m quadratischer Rest oder Nichtrest ist von n', ist $\mu_0(m, n') \equiv 0$ oder $\equiv \frac{1}{2}\chi(n') \pmod{2}$.

Indem man n' als ungerade Primzahl p voraussetzt, in welcher Voraussetzung $\chi(n') = 2$ und $\mu_0(m, n') = \mu(m, p)$ wird, kommt man von hier offenbar auf das Gaufssche Lemma zurück.

Indessen läfst sich die Bedeutung des Zeichens $\mu_0(m, n')$ noch anders fassen und führt dann zur Verallgemeinerung dieses Lemmas. Die Kongruenzen (39) sind nämlich völlig gleichbedeutend mit den folgenden:

$$m \cdot dr_i \equiv \varepsilon_i \cdot dr_i' \pmod{n}$$
$$\left(i = 1, 2, 3 \cdots \frac{1}{2}\varphi(n')\right)$$

und in den letzteren bilden nun sowohl die Faktoren dr_i als auch die Reste dr_i' die gesamte zum Teiler d gehörige Klasse der Zahlen (35);

mithin bedeutet $\mu_0(m, n')$ die Anzahl derjenigen Produkte aus m und den Zahlen der zu d gehörigen Klasse, deren absolut kleinste Reste (mod. n) negativ sind. Da nun die Zahlen (35) sich aus den zu den verschiedenen Teilern d gehörigen Klassen zusammensetzen, so wird die auf diese Teiler d bezw. auf die zugehörigen Quotienten $\frac{n}{d} = n'$ bezogene Summe

$$\sum_{n'} \mu_0(m, n')$$

die Anzahl der Produkte

$$(41) \qquad 1 \cdot m,\ 2 \cdot m,\ 3 \cdot m,\ \cdots \frac{n-1}{2} \cdot m$$

bedeuten, deren absolut kleinste Reste (mod. n) negativ sind. Nennen wir also diese Anzahl $\mu(m, n)$, so ist

$$(42) \qquad \mu(m, n) = \sum_{n'} \mu_0(m, n').$$

So oft aber m quadratischer Rest von n' ist, ist das entsprechende Glied dieser Summe gerade, im andern Falle kongruent $\frac{1}{2}\chi(n')$ (mod. 2), also findet sich

$$\mu(m, n) \equiv \sum \frac{1}{2}\chi(n') \pmod{2},$$

wo die neue Summation nur noch auf diejenigen Teiler $n' > 2$ von n zu erstrecken ist, in Bezug auf welche m quadratischer Nichtrest ist. Ferner ist $\chi(n')$ stets eine höhere Potenz von 2, mithin $\frac{1}{2}\chi(n')$ eine gerade Zahl, so oft n' aus mehr als einer Primzahl besteht; daher braucht man die Summation in voriger Kongruenz nur über diejenigen der genannten Teiler n' von n auszudehnen, welche Primzahlpotenzen, also Potenzen solcher Primfaktoren von n sind, in Bezug auf welche m quadratischer Nichtrest ist; der bezügliche Wert von $\chi(n')$ ist 2, mithin liefert jede solche Potenz eine Einheit zur Summe. Ist daher p jeder Primfaktor von n, für welchen m quadratischer Nichtrest ist, und geht er genau a-mal in n auf, so giebt es a entsprechende Primzahlpotenzen n', die zusammen a Einheiten zur Summe liefern. Man erkennt hieraus, dafs man $\mu(m, n) \equiv A$ (mod. 2) setzen darf, wenn A die gesamte Anzahl aller (gleichen oder verschiedenen) Primfaktoren p von n bedeutet, in Bezug auf welche m qudratischer Nichtrest, $\left(\frac{m}{p}\right) = -1$ ist. Der Definition des Jacobischen Symbols gemäfs ist aber offenbar

$$\left(\frac{m}{n}\right) = (-1)^A$$

und folglich besteht nach der vorigen Kongruenz die Gleichheit

(43) $$\left(\frac{m}{n}\right) = (-1)^{\mu(m,n)}$$

d. h. das Scheringsche oder das verallgemeinerte Gaufssche Lemma:

Ist m relativ prim gegen die ungerade Zahl n und bedeutet $\mu(m, n)$ die Anzahl der absolut kleinsten Reste der Reihe (41), welche negativ sind, so bestimmt sich der Wert des **Jacobi**schen Symbols $\left(\frac{m}{n}\right)$ durch die Formel (43), ist also $+1$ oder -1, jenachdem $\mu(m, n)$ gerade oder ungerade ist.

5. Nunmehr wollen wir zeigen, wie die gewonnenen Kriterien nutzbar gemacht werden können, den quadratischen Charakter einer Zahl m in Bezug auf eine dazu relativ prime Zahl n zu bestimmen. Wie bereits bemerkt, darf man dabei die letztere als eine ungerade Primzahl voraussetzen; aber dem in (15) ausgesprochenen Satze zufolge genügt es ferner, den Fall zu untersuchen, wo auch m eine unzerlegbare Zahl ist, und da sie positiv oder negativ, gerade oder ungerade sein kann, kommt alles darauf hinaus, den Wert der folgenden drei Symbole festzustellen:

(44) $$\left(\frac{-1}{p}\right),\quad \left(\frac{2}{p}\right),\quad \left(\frac{q}{p}\right),$$

in deren letztem q eine von p verschiedene ungerade Primzahl bedeutet. Den Wert des letztern giebt ein Satz, der seiner eigentümlichen Natur nach von Legendre, welchem man auch seinen eleganten formalen Ausdruck verdankt, als Reziprozitätsgesetz der quadratischen Reste benannt worden ist, weil er zunächst nur den Wert des Symbols $\left(\frac{q}{p}\right)$ auf denjenigen des „reziproken" Symbols $\left(\frac{p}{q}\right)$ zurückführen läfst; wie derselbe Wert auf solche Weise dann wirklich ermittelt werden kann, wird später erhellen. Dieser Satz, bei weitem einer der schönsten und interessantesten der ganzen Zahlentheorie, wird ausgesprochen durch die Formel

(45) $$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Diejenigen Sätze, welche den Wert der beiden Symbole $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ angeben, heifsen gewöhnlich die Ergänzungssätze zum Reziprozitätsgesetze. Sie sind bereits Fermat bekannt gewesen, wie aus einem in J. Wallis' *W.* II, p. 857 enthaltenen Briefe von Fermat an Kenelm Digby, sowie aus einem Briefe von Frénicle an Fermat (s. des Letztern *varia op. math.*, *Tolosae* 1679, p. 168) hervorgeht; auch kannte Fermat bereits einzelne Sätze über den quadratischen Charakter anderer Zahlen. Den ersten der Ergänzungs-

sätze bewies aber zuerst L. Euler (*Opusc. analyt.* 1, 1783, p. 64, 121 (135) oder *Comm. Ar. coll.* 1, p. 477 (§§ 23, 30), 487 (§ 31); s. auch *Petrop. Comm. nov.* 5, 1754/55, p. 3 oder *Comm. Ar. coll.* 1, p. 210). Er ergiebt sich unmittelbar aus dem Eulerschen Kriterium; denn setzt man in demselben $m = -1$, so nimmt es die Gestalt an:

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p},$$

aus welcher Kongruenz, wie schon mehrfach bemerkt, die Gleichung

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \tag{46}$$

hervorgeht. In Worten: Die Zahl -1 ist quadratischer Rest von jeder Primzahl p von der Form $4z+1$, quadratischer Nichtrest von jeder Primzahl p von der Form $4z+3$.

Dieser Satz kann auch direkt aus der Quelle, welcher das Eulersche Kriterium selbst entquoll, aus der Betrachtung associierter Zahlen geschöpft werden (s. Gaufs, *Disqu. Ar. art.* 109). Ist nämlich m ein quadratischer Rest (mod. p), so wird es die associierte Zahl m' ebenfalls sein, da aus $mm' \equiv 1 \pmod{p}$ nach (14) und (15)

$$\left(\frac{mm'}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{m'}{p}\right) = \left(\frac{1}{p}\right) \quad \text{d. h.} \quad = 1$$

und wegen $\left(\frac{m}{p}\right) = 1$ auch $\left(\frac{m'}{p}\right) = 1$ sich ergiebt. Diese zu m associierte Zahl m' kann aber nur dann mit m kongruent sein, wenn $m^2 \equiv 1 \pmod{p}$, d. h., da diese Kongruenz nur die Wurzeln $+1$, -1 hat, wenn der quadratische Rest m gleich 1 oder -1 ist. Sind diese Zahlen, deren erste stets quadratischer Rest ist, beide solche Reste, so ist, da die übrigen quadratischen Reste paarweise vorhanden sind, die Anzahl $\frac{p-1}{2}$ aller quadratischen Reste eine gerade Zahl; ist aber -1 quadratischer Nichtrest von p, so mufs die Anzahl $\frac{p-1}{2}$ aller quadratischen Reste eine ungerade Zahl sein. Daher ist p von der Form $4z+1$ oder $4z+3$, jenachdem -1 quadratischer Rest oder Nichtrest von p ist.

Auch aus Fermats Satz erschliefst man dasselbe mittels des Begriffs der primitiven Wurzeln, den wir für diesen Zweck hier wie schon in Nr. 7 des vor. Kap. vorwegnehmen; später werden wir zeigen, dafs es primitive Wurzeln (mod. p) d. h. Zahlen giebt, für welche die $(p-1)^{\text{te}}$ Potenz die niedrigste ist mit dem Reste 1 (mod. p), wie ihn nach dem Fermatschen Satze die $(p-1)^{\text{te}}$ Potenz jeder zu p primen Zahl giebt. Sei g eine solche primitive Wurzel (mod. p). Aus

$$g^{p-1} - 1 = \left(g^{\frac{p-1}{2}} - 1\right)\left(g^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}$$

folgt dann

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}; \tag{47}$$

also mufs g quadratischer Nichtrest von p sein, denn, wäre $g \equiv x^2$, so würde der Bedeutung von g zuwider $g^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1$ sein; wegen (47) wird daher -1 quadratischer Rest oder Nichtrest von p sein, jenachdem $\frac{p-1}{2}$ gerade oder ungerade d. h. jenachdem p von der Form $4z+1$ oder $4z+3$ ist.

6. Den andern der Ergänzungssätze bewies zuerst Lagrange (*Nouv. Mém. de l'Ac. de Berlin*, 1775, p. 349, 351), demnächst Gaufs (*Disqu. Ar. art.* 112—116), indem er sich zu diesem Zwecke der allgemeinen Induktion bedient, sowie in seiner Abhandlung *theorem. arithmetici demonstratio nova*, W. II, p. 1 mittels seines oben gegebenen Lemmas. In der That, setzt man im letztern $m = 2$ voraus, so werden die Zahlen (31) die folgenden:

$$2,\ 4,\ 6,\ \ldots,\ (p-1); \tag{48}$$

bestimmt man nun die ganze Zahl μ durch die Bedingung, dafs

$$p - 1 - 2\mu < \frac{p}{2} < p + 1 - 2\mu \tag{49}$$

sein solle, so werden die μ Zahlen

$$p+1-2\mu,\quad p+3-2\mu,\ \ldots,\ (p-1)$$

die sämtlichen Zahlen der Reihe (48) sein, welche $> \frac{p}{2}$, deren absolut kleinste Reste (mod. p) mithin negativ sind, und es ergiebt sich nach dem Gaufsschen Lemma

$$\left(\frac{2}{p}\right) = (-1)^{\mu}.$$

Aus den Ungleichheiten (49) aber folgen diese anderen:

$$\frac{p-2}{4} < \mu < \frac{p+2}{4},$$

nach welchen $\mu = \left[\frac{p+2}{4}\right]$, oder auch, da p ungerade ist,

$$\mu = \left[\frac{p+1}{4}\right]$$

ist. Demnach findet sich der zweite Ergänzungssatz ausgedrückt durch die Formel:

$$\left(\frac{2}{p}\right) = (-1)^{\left[\frac{p+1}{4}\right]}. \tag{50}$$

Nun findet sich

$$\text{für } p = 8z+1: \quad \left[\frac{p+1}{4}\right] = 2z, \qquad \frac{p^2-1}{8} = 8z^2 + 2z,$$

$$\text{„} \quad p = 8z+3: \quad \left[\frac{p+1}{4}\right] = 2z+1, \qquad \frac{p^2-1}{8} = 8z^2 + 6z + 1,$$

$$\text{„} \quad p = 8z+5: \quad \left[\frac{p+1}{4}\right] = 2z+1, \qquad \frac{p^2-1}{8} = 8z^2 + 10z + 3,$$

$$\text{„} \quad p = 8z+7: \quad \left[\frac{p+1}{4}\right] = 2z+2, \qquad \frac{p^2-1}{8} = 8z^2 + 14z + 6;$$

da hiernach $\left[\frac{p+1}{4}\right]$ und $\frac{p^2-1}{8}$ immer zugleich gerade bezw. ungerade sind, läfst sich die Formel (50) auch durch die andere:

$$(51) \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

ersetzen und als Satz folgendermafsen aussprechen:

Die Zahl 2 ist quadratischer Rest von jeder Primzahl von einer der Formen $8z+1$, $8z+7$, quadratischer Nichtrest von jeder Primzahl von einer der Formen $8z+3$, $8z+5$. *)

7. Bevor wir weitergehen, dehnen wir die erhaltenen Formeln auf den Fall zusammengesetzter Moduln aus. Sei $P = pp'p'' \dots$ eine aus beliebig vielen, gleichen oder ungleichen Primfaktoren zusammengesetzte, ungerade Zahl. Aus den Gleichungen

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{-1}{p'}\right) = (-1)^{\frac{p'-1}{2}}, \quad \left(\frac{-1}{p''}\right) = (-1)^{\frac{p''-1}{2}}, \dots$$

folgt sogleich für das Jacobische Symbol $\left(\frac{-1}{P}\right)$ der Wert

$$(52) \qquad \left(\frac{-1}{P}\right) = (-1)^{\frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \cdots}.$$

Nun kann man schreiben:

$$P = ((p-1)+1)\,((p'-1)+1)\,((p''-1)+1) \dots;$$

die Teile $p-1, p'-1, p''-1, \dots$ sind sämtlich gerade, Produkte von zweien oder mehreren von ihnen also teilbar durch 4, sodafs man, die rechte Seite der Gleichung entwickelnd,

$$P - 1 = 4z + (p-1) + (p'-1) + (p''-1) + \cdots$$

also

*) Andere Beweise dieses Satzes gab Gaufs, *Disqu. Ar. art.* 262, auf Grund der Theorie der quadratischen Formen, Lebesgue mit den Hilfsmitteln der Lehre von der Kreisteilung. S. ferner einen Beweis von Petersen unten in Nr. 20.

$$\frac{P-1}{2} = 2z + \frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \cdots$$

erhält. Demnach läſst sich die Formel (52) auch schreiben, wie folgt:

$$(53) \qquad \left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}},$$

eine Gleichung, welche die Verallgemeinerung der Formel (46) ist.

Desgleichen folgt aus den Gleichungen

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, \quad \left(\frac{2}{p'}\right) = (-1)^{\frac{p'^2-1}{8}}, \quad \left(\frac{2}{p''}\right) = (-1)^{\frac{p''^2-1}{8}}, \ldots$$

zunächst diese andere:

$$(54) \qquad \left(\frac{2}{P}\right) = (-1)^{\frac{p^2-1}{8} + \frac{p'^2-1}{8} + \frac{p''^2-1}{8}} + \cdots.$$

Nun ist

$$P^2 = ((p^2-1)+1)\,((p'^2-1)+1)\,((p''^2-1)+1)\ldots;$$

hier sind die Teile p^2-1, p'^2-1, $p''^2-1, \ldots$, da $p, p', p'', \ldots$ ungerade sind, sämtlich durch 8, Produkte aus zwei oder mehreren von ihnen also durch 64 teilbar, sodaſs man, die rechte Seite entwickelnd,

$$P^2 - 1 = 64z + (p^2-1) + (p'^2-1) + (p''^2-1) + \cdots$$

also

$$\frac{P^2-1}{8} = 8z + \frac{p^2-1}{8} + \frac{p'^2-1}{8} + \frac{p''^2-1}{8} + \cdots$$

erhält und die Formel (54) durch diese andere:

$$(55) \qquad \left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$$

ersetzen kann, welche die Verallgemeinerung der Formel (51) ausmacht. Nach der oben gemachten Festsetzung, nach welcher $\left(\frac{2}{-P}\right) = \left(\frac{2}{P}\right)$ sein soll, darf in der letztern Formel die bisher immer positiv gedachte Zahl P auch negativ sein.

Um den Gang späterer Betrachtungen nicht zu stören, fügen wir hier auch sogleich das verallgemeinerte Reziprozitätsgesetz an. Seien

$$P = pp'p''\ldots, \qquad Q = qq'q''\ldots$$

zwei aus beliebig vielen, gleichen oder ungleichen Primfaktoren zusammengesetzte, relativ prime, positive ungerade Zahlen. Angenommen, das Reziprozitätsgesetz gelte für jedes aus einem Primfaktor von P und einem Primfaktor von Q bestehende Paar, so gilt es auch für P, Q selbst, d. h. es gilt die Formel:

$$(56) \qquad \left(\frac{P}{Q}\right) \cdot \left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

Um sich hiervon zu überzeugen, bemerke man zunächst, dafs nach der Definition des Jacobischen Symbols

$$\left(\frac{P}{Q}\right)=\left(\frac{P}{q}\right)\cdot\left(\frac{P}{q'}\right)\cdot\left(\frac{P}{q''}\right)\cdots$$

folglich wegen (15)

$$\left(\frac{P}{Q}\right)=\prod\left(\frac{p}{q}\right)$$

ist, wenn man die rechts durch das Zeichen Π angedeutete Multiplikation auf jedes der bezeichneten Paare bezieht; in gleicher Weise kommt

$$\left(\frac{Q}{P}\right)=\prod\left(\frac{q}{p}\right)$$

also

$$\left(\frac{P}{Q}\right)\cdot\left(\frac{Q}{P}\right)=\prod\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$$

und nach dem vorausgesetzten Reziprozitätsgesetze

$$\left(\frac{P}{Q}\right)\cdot\left(\frac{Q}{P}\right)=(-1)^{\Sigma\frac{p-1}{2}\cdot\frac{q-1}{2}}, \tag{57}$$

wo nun die Summe rechts auf alle gedachten Paare erstreckt werden mufs. Diese Summe ist dann aber nichts anderes als das entwickelte Produkt

$$\left(\frac{p-1}{2}+\frac{p'-1}{2}+\frac{p''-1}{2}+\cdots\right)\left(\frac{q-1}{2}+\frac{q'-1}{2}+\frac{q''-1}{2}+\cdots\right),$$

dessen erster Faktor nach dem Obigen mit $\frac{P-1}{2}$, dessen zweiter Faktor ebenso mit $\frac{Q-1}{2}$ (mod. 2) kongruent ist; somit darf die Formel (57) auch, wie behauptet, ersetzt werden durch diese andere:

$$\left(\frac{P}{Q}\right)\cdot\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

Hiernach darf man die letzte Formel **für je zwei positive ungerade Zahlen P, Q ohne gemeinsamen Teiler** als giltig betrachten, sobald das **Legendre**sche Reziprozitätsgesetz **für je zwei ungerade Primzahlen** bewiesen sein wird.

Auch kann man das allgemeine Gesetz dann noch umfassender aussprechen, sodafs es sich auch auf negative Zahlen erstreckt. Sind nämlich M, N zwei beliebige ungerade Zahlen ohne gemeinsamen Teiler, P, Q ihre resp. Absolutwerte, so kann man, unter δ, ε positive oder negative Einheiten verstehend,

$$M=\delta P,\qquad N=\varepsilon Q$$

setzen und findet zunächst

$$\left(\frac{M}{N}\right)\cdot\left(\frac{N}{M}\right)=\left(\frac{\delta P}{Q}\right)\cdot\left(\frac{\varepsilon Q}{P}\right) \tag{58}$$

also auch gleich

$$\left(\frac{\delta}{Q}\right)\left(\frac{\varepsilon}{P}\right)\cdot\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right).$$

Nun ist offenbar mit Rücksicht auf (53)

$$\left(\frac{\varepsilon}{P}\right)=\varepsilon^{\frac{P-1}{2}}=(-1)^{\frac{\varepsilon-1}{2}\cdot\frac{P-1}{2}},$$

$$\left(\frac{\delta}{Q}\right)=\delta^{\frac{Q-1}{2}}=(-1)^{\frac{\delta-1}{2}\cdot\frac{Q-1}{2}};$$

wendet man zudem die Formel (56) an, so findet man folgende allgemeinste Reziprozitätsgleichung:

$$\left(\frac{M}{N}\right)\cdot\left(\frac{N}{M}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}+\frac{\varepsilon-1}{2}\cdot\frac{P-1}{2}+\frac{\delta-1}{2}\cdot\frac{Q-1}{2}}, \tag{59}$$

wofür man, wie leicht zu übersehen, auch die Formel

$$\left(\frac{M}{N}\right)\cdot\left(\frac{N}{M}\right)=(-1)^{\frac{M-1}{2}\cdot\frac{N-1}{2}+\frac{\delta-1}{2}\cdot\frac{\varepsilon-1}{2}} \tag{60}$$

schreiben darf, die zugleich mit dem **Legendre**schen Reziprozitätsgesetze bewiesen ist.

Man sieht hieraus, daſs, wenn die Formel (56) für je zwei positive ungerade Zahlen ohne gemeinsamen Teiler besteht, sie auch für zwei derartige Zahlen, deren wenigstens eine positiv ist, bestehen bleibt.

Man darf aber der diesen letzten Resultaten voraufgeschickten Bemerkung gemäſs — und wir werden bald in diesem Sinne von ihr Gebrauch machen — auch sagen: daſs, wenn das Legendresche Gesetz giltig gedacht wird für je zwei Primzahlen unterhalb einer gegebenen Grenze, auch die Formel (56) giltig sein müsse für je zwei, nicht gleichzeitig negative, Zahlen P, Q, welche nur aus solchen Primzahlen zusammengesetzt sind.

8. Indem wir uns nun dazu wenden, die Beweise zu betrachten, welche man für das Reziprozitätsgesetz gegeben hat, beginnen wir mit einigen bezüglichen geschichtlichen Bemerkungen (s. dazu Kronecker, *Bemerkungen zur Geschichte des R. G.*, *Berl. Monatsber.* 1875, p. 267). Das Gesetz ist in der eleganten Form, wie es die Gleichung (45) ausspricht, zuerst von Legendre gegeben worden in seinem *essai sur la théorie des nombres*, 1798, p. 186, nachdem er es in seinem wesentlichen Inhalte ohne Anwendung des Symbols $\left(\frac{m}{p}\right)$ bereits in einer Abhandlung: *recherches d'analyse indéterminée*, in *Hist. de l'Acad. de Paris*, 1785, p. 465 (516, 517) aufgestellt und auch zu beweisen versucht hatte. Dieser, auf die Betrachtung quadratischer Formen

gegründete Beweis läſst aber in einem wesentlichen Punkte zu wünschen, indem er die Existenz von Primzahlen voraussetzt, die in gewissen arithmetischen Progressionen enthalten sind, ein Umstand, dessen thatsächliche Richtigkeit erst viel später durch Lejeune Dirichlet (s. Kap. 2, Nr. 7) auf Grund eben des Reziprozitätsgesetzes selbst festgestellt worden ist; und zwar haftet dieser Mangel auch der Legendreschen Darstellung seines Beweises an der späteren Stelle an, wo nur die Voraussetzungen über jene Existenz in etwas beschränkt, doch nicht völlig beseitigt sind. Wenn somit Legendre sich nicht als Denjenigen betrachten durfte, dem der erste Beweis des interessanten Satzes gelungen war, so sah er sich doch wenigstens als seinen Entdecker an und beklagte sich in einem an Jacobi gerichteten Briefe über Gauſs, daſs dieser im Jahre 1801 die Entdeckung des Gesetzes sich habe zuschreiben wollen. Letzteres hat nun Gauſs eigentlich nicht gethan; spricht er sich in seinen *Disqu. arithm. art.* 151, wo er über die das Reziprozitätsgesetz betreffenden Arbeiten seiner Vorgänger berichtet, auch weniger entschieden über Legendre's Verdienste aus, wie in der späteren Stelle: Pro primo hujus elegantissimi theorematis inventore ill. Legendre absque dubio habendus est (*W.* II, p. 4, s. auch p. 152), so erkennt er doch mit den Worten: Post Eulerum clar. Legendre eidem argumento operam navavit in egregia tractatione Rech. d'anal. indét. etc., ubi pervenit ad theorema, quod si rem ipsam spectas, cum theoremate fundamentali idem est, durchaus die Entdeckung Legendres an und vindiziert sich selbst nur einen einfacheren Ausdruck desselben, wenn er schreibt: theorema fundamentale . . . in eadem forma simplici, in qua supra propositum est, a nemine hucusque fuit prolatum.

Übrigens kann Legendre auch nicht als Entdecker des Reziprozitätsgesetzes anerkannt werden, eine Ehre, welche vielmehr L. Euler zukommt. Schon Gauſs und auch Legendre haben bemerkt, daſs vor ihnen bereits Euler spezielle Fälle des umfassenden Gesetzes gekannt, wenngleich nur auf induktivem Wege erhalten hat, während seine Bemühungen, sie zu beweisen, nicht von Erfolg gekrönt worden sind; Gauſs zitiert zwei solcher Abhandlungen Eulers: *Novae demonstr. circa divisores numerorum formae* x^2+ny^2, *N. Act. Petrop.* 1, 1775, p. 47, und *de criteriis aequationis* $fx^2+gy^2=hz^2$ *etc.* in *Opusc. anal.* 1, 1783. Aber viel früher schon hat derselbe Forscher in seiner Abhandlung *theoremata circa divisores numerorum in hac forma* $pa^2 \pm qb^2$ *contentorum, Comm. Ac. Petrop.* 1744/46, p. 151 oder *Comm. Ar. coll.* 1, p. 35, induktorische Sätze über die Primteiler der Formen $a^2 \pm Nb^2$ und ihre Verteilung in gewisse Linearformen $4Nm \pm \alpha$ angegeben, welche im Grunde das Reziprozitätsgesetz in sich enthalten; ganz deutlich aber und in einer Form, die sich leicht in die von Gauſs gegebene umsetzen läſst, sprach er

dasselbe am Schlusse einer andern Abhandlung aus: *Observationes circa divisionem quadratorum per numeros primos, Opusc. anal.* 1, 1783, p. 64 oder *Comm. Ar. coll.* 1, p. 477 (486), welche merkwürdiger Weise sowohl von Gaufs wie von Legendre übersehen worden ist, obwohl beide Forscher andere Abschnitte dieses Sammelwerkes zitieren. Die bezügliche Stelle lautet folgendermafsen:

Existente s numero quocunque primo, dividantur tantum quadrata imparia 1, 9, 25, 49 etc. per divisorem $4s$, notenturque residua, quae omnia erunt formae $4q+1$, quorum quodvis littera α indicetur, reliquorum autem numerorum formae $4q+1$, qui inter residua non occurrunt, quilibet littera $\mathfrak{A}$ indicetur; quo facto si fuerit

divisor numerus primus,	tum est
formae $4ns+\alpha$	$+s$ residuum, et $-s$ residuum,
" $4ns-\alpha$	$+s$ residuum, et $-s$ non-residuum,
" $4ns+\mathfrak{A}$	$+s$ non-residuum, et $-s$ non-residuum,
" $4ns-\mathfrak{A}$	$+s$ non-residuum, et $-s$ residuum.

Bezeichnet man hier den gedachten Primteiler mit p und beschränkt sich nur auf den quadratischen Charakter von $+s$, so besagt dieser Ausspruch Euler's nichts Anderes als dies: jenachdem $(-1)^{\frac{p-1}{2}}\cdot p$ quadratischer Rest oder Nichtrest ist von s, sei s quadratischer Rest oder Nichtrest von p, und stimmt also genau mit Gaufs' Fassung des Reziprozitätsgesetzes (*Disqu. Ar. art.* 131) überein, welche lautet:

Si p est numerus primus $4n+1$, erit $+p$, si vero p formae $4n+3$, erit $-p$ residuum vel non-residuum cujusvis numeri primi, qui positive acceptus ipsius p est residuum vel non-residuum.

Gebührt hiernach Euler die Ehre, den Inhalt des Reziprozitätsgesetzes zuerst vollständig erkannt zu haben, so hat Gaufs das sehr viel höhere Verdienst, es zuerst völlig streng erwiesen zu haben (*Disqu. Ar. art.* 130—151). Nachdem er bereits im März 1795 ganz unabhängig von den Arbeiten seiner Vorgänger, die ihm unbekannt waren, auf dem Wege der Induktion zu dem Reziprozitätsgesetze gekommen war, bedurfte es der angestrengtesten, wiederholten Bemühungen eines ganzen Jahres (s. dazu Gaufs' *W.* 2, p. 4), bis jener Beweis desselben ihm endlich im April 1796 gelang, nachdem er einen später anzumerkenden Satz, der den eigentlichen Nerv des Beweises ausmacht, am 8. April dieses Jahres festgestellt hatte (Gaufs' *W.* 1, p. 475). Doch hat es bei diesem einen Beweise des Reziprozitätsgesetzes nicht sein Bewenden gehabt. Dies Gesetz ist nicht nur einer der schönsten Sätze der ganzen Zahlentheorie, sondern er ist auch einer der wichtigsten; er ist dies und ist es mehr und mehr geworden. Er ist es, weil er nicht nur für die Lehre von den quadratischen Resten das theorema fundamentale bedeutet, wie Gaufs ihn genannt hat, sondern weil er in den verschiedensten Ge-

bieten der höheren Arithmetik eine wesentlich grundlegende Rolle behauptet; und er ist es geworden, weil die Bemühungen der Forscher, ihn zu beweisen, nach mehreren Richtungen hin für die Entwicklung und tiefere Erfassung der Wissenschaft zum Ausgangspunkte geworden sind. Es findet hier selbst eine gewisse Reziprozität statt: boten die Fortschritte der Zahlentheorie, wie sie schon durch Gaufs mit der Lehre von der Kreisteilung, mit der Theorie der höheren Kongruenzen, der höheren Potenzreste u. a. erzielt wurden, immer neue Beweismittel dar, jenen interessanten Hauptsatz zu begründen, so eröffneten die neuen Gesichtspunkte, von welchen aus dies geschah, stets tiefere Blicke in die Grundlagen des Gesetzes oder in die Verkettung der verschiedenen Zweige der Zahlentheorie, oder auch Wege, auf denen ähnliche Probleme höherer Art, die Beweise der Reziprozitätsgesetze der höheren Potenzreste u. a. m. erreicht werden konnten, und förderten somit immer auf's neue die Wissenschaft. Solche Erwägungen waren es wesentlich (s. darüber Gaufs' *W.* 2, p. 49, 50 und 159), welche schon Gaufs selbst zu stets erneuten Versuchen, das Reziprozitätsgesetz zu beweisen, geführt und uns im Ganzen sieben (oder acht) ganz verschiedene Beweise desselben geschenkt haben. Aber bis auf die neueste Zeit sind andere Forscher ihm darin nachgefolgt, und so kennt man gegenwärtig nachgerade eine grofse Menge von Beweisen des Gesetzes, von denen nach dem Gesagten nicht ohne einige Berechtigung geäufsert werden darf, dafs ihre Folge „die gleichzeitige Geschichte unserer gesamten Mathematik im Kleinen wiederspiegelt“ (s. Baumgart, *über das quadratische Reziprozitätsgesetz, Ztschr. f. Math. u. Phys.* 1885, hist.-liter. Abt. p. 169, in der Einleitung). Die nachstehende Zusammenstellung giebt die ganze Reihe der bisher gegebenen Beweise, soweit sie dem Verfasser bekannt geworden sind, in chronologischer Anordnung an:

Chronologische Tabelle der Beweise des Reziprozitätsgesetzes.

1.	Gaufs, 1. Beweis, *Disqu. Ar. art.* 135 ff., 1801 (1796).	Induktion.
2.	„ , 2. „ , „ „ „ 257 ff., 1801.	Quadr. Formen.
3.	„ , 7. u. 8. Beweis, *W.* 2, p. 233 (1801)	höh. Kongruenzen.
4.	„ , 3. Beweis, *Comm. Gott.* 16, 1808; *W.* 2, p. 1,	Gaufs. Lemma.
5.	„ , 4. „ , *Comm. Gott. rec.* 1, 1809; *W.* 2, p. 9.	Kreisteilung.
6.	„ , 5. „ , ebend, 4. 1818; *W.* 2, p. 47.	Gaufs. Lemma.
7.	„ , 6. „ , an derselben Stelle.	Kreisteilung.
8.	Cauchy, *Bull. de Férussac* 12, 1829, p. 205.	desgl.
9.	Jacobi, Journ. f. Math. 30, p. 172, vgl. 35, p. 273.	desgl.
10.	Eisenstein, Journ. f. Math. 27, 1844, p. 322.	desgl. (arithm.)
11.	„ , „ „ „ 28, 1844, p. 41.	desgl.
12.	„ , „ „ „ 28, 1844, p. 246.	G. Lemma, (geom.)
13.	„ , „ „ „ 29, 1845, p. 257.	Kreist. $\left(\frac{\sin pv}{\sin v}\right)$.

14. Liouville, *Journ. de Math.* 12, 1847, p. 95.	Kreist.
15. Lebesgue, ebendas. p. 457.	desgl. (arithm.)
16. Schaar, *Bulletin Belgique*, 14 I, 1847, p. 79.	G. Lemma.
17. Genocchi, *Ac. R. Belg., mém. couronnés*, 25, 1853 (52).	desgl.
18. Lebesgue, *Par. Comptes R.* 51, 1860, p. 9.	höh. Kongr.
19. Kummer, zwei Beweise, *Abh. Berl. Ak.* 1861.	Quadr. Formen.
20. Stern, *Gött. Nachr.* 1870, p. 237.	G. Lemma.
21. Zeller, *Berl. Monatsber.* 1872, p. 846.	desgl.
22. Zolotareff, *Nouv. Ann. de Math.* (2) 11, 1872, p. 354.	Permutationen.
23. Kronecker, *Berl. Monatsber.* 1876, p. 301.	Induktion.
24. Bouniakowsky, *Bull. St. Pét.* 22, 1876.	variirtes G. L.
25. Schering, *Gött. Nachr.* 1879, p. 217. *P. C. R.* 88, p. 1073.	G. Lemma.
26. Petersen, *Amer. Journ.* 2, 1879, p. 217, *Zeuthen*, *Tidskr.* 1879, p. 86.	var. G. L.
27. Voigt, *Ztschr. f. Math. u. Phys.* 26, 1881, p. 134.	G. Lemma.
28. Busche, *Dissertation*, *Göttingen* 1883.	desgl., Hilfssatz.
29. Kronecker, *Berl. Sitzgsber.* 1884, p. 645.	G. Lemma.
30. Gegenbauer, *Wiener Ber.* 1884, p. 1026; 1885, p. 876.	desgl.
31. Kronecker, *Berl. Sitzgsber.* 1885, p. 117.	desgl.
32. „ , „ „ 1885, p. 383, 1045.	desgl.
33. Hermes, *Arch. f. Math. u. Phys.* (2) 5, 1887, p. 190.	Induktion.
34. Lerch, *Teixeira Journ.* 8, 1887, p. 137.	G. Lemma.
35. Busche, *J. f. Math.* 103, 1888, p. 118.	var. G. Lemma.
36. „ , „ „ „ 106, 1890, p. 65.	G. Lemma.
37. Lucas, *Bull. St. Pét.*, *nouv. sér.* 1, 1890. *Assoc. franç.*, *Limoges*, 19, 1890, p. 147.	desgl.
38. Franklin, *Mess. of Math.* (2) 19, 1890, p. 176.	desgl.
39. Fields, *Amer. Journ.* 13, 1891, p. 189.	desgl.
40. Gegenbauer, *Wiener Ber.* 100, 1891, p. 855.	desgl.
41. Schmidt, *J. f. Math.* 111, 1893, p. 107, drei Beweise,	
erster Beweis:	desgl.
zweiter Beweis:	desgl. (versteckt).
dritter Beweis:	Induktion.
42. Gegenbauer, *Wiener Ber.* 103, 1894, p. 285.	G. Lemma.
43. A. S. Bang, *N. Tidsskr. for Math.* 5 B, 1894, p. 92.	Induktion.
44. Busche, *Hamburger Mitt. III*, 6, 1896, p. 233.	var. G. L. (geom.).
45. Lange, drei Beweise, *Leipz. Ber.* 48, 1896, p. 629. „ „ 49, 1897, p. 607.	G. Lemma.

Was die angegebene Chronolgie der Gaufsischen Beweise betrifft, welche wir in gewohnter Weise nach der Reihenfolge ihrer Publikation als ersten, zweiten Beweis u. s. f. bezeichnet haben, so beruht sie auf folgender Erwägung. Dem ersten Beweise fügt Gaufs (*D. A. art.* 151) die Zusage bei: ceterum infra duas alias demonstrationes ejusdem gravissimi theorematis trademus etc.; einer von diesen Beweisen findet sich in der That in *art.* 262 desselben Werkes. Nach Kronecker's, wie mir scheint, irriger Meinung wäre nun der zweite jener Beweise sein „vierter“, der in der *summatio quar. serier. singul.* enthaltene, der Kreisteilung zugehörige Beweis, weil nach

Dedekinds Aussage im Gaufsschen Nachlasse ein Fragment „*Sectio octava*“ vorhanden sei, dessen wesentlicher Inhalt später in jene Abhandlung übergegangen ist. Dem ist aber entgegenzuhalten, dafs nach desselben Forschers Aussage sich dort ein anderes Fragment vorfindet mit dem Titel: *Disquis. generales de congruentiis, Analysis Residuorum, caput octavum*, welches einem umfangreichen, durch eine gänzliche Umarbeitung in die *Disquisitiones arithmeticae* übergegangenen Manuskripte entnommen sei; in ihm sind der „siebente“ und „achte“ Beweis enthalten mit der ausdrücklichen Zählung: haec igitur est tertia theorematis fundamentalis completa demonstratio ... At ex eodem fonte sed via opposita quartam deducamus. So dürfte eher wohl dieser Doppelbeweis der andere der von Gaufs im *art.* 151 gemeinten beiden Beweise sein. Es scheint mir daher auch zweifelhaft, ob Kronecker Recht hat, wenn er meint, Gaufs' „vierter Beweis“ gehöre zu den „drei anderen Beweisen“, welche *W.* 2, p. 153 als vor dem „dritten“ Beweise gefunden erwähnt werden; ohne Zweifel hat hier vielmehr Gaufs jenen Doppelbeweis eben als dritten und vierten gezählt. Wäre es an sich auch wohl möglich, dafs jener „vierte“ Beweis, aus Gaufs' Beschäftigung mit der Kreisteilung entsprungen, vor dem „dritten“ von ihm gefunden worden ist, so liegt doch dafür in seinen Aussagen nicht der geringste Anhaltepunkt vor, und man wird daher wohl die Chronologie dieser folgenden Beweise ganz nach den Daten ihrer Veröffentlichung zu bestimmen haben.

In der letzten Kolonne der voraufgehenden Tabelle ist kurz die Grundlage bezeichnet, auf welcher die einzelnen Beweise sich erbauen. Man sieht, dafs sie sich sämtlich etwa in fünf Kategorieen verteilen, die bereits durch die Gaufsischen Beweise vorgezeichnet sind. Die erste Kategorie wird durch den ersten Gaufsischen Beweis bezeichnet, der der einzige ist, welcher ganz innerhalb der elementaren Theorie der quadratischen Reste verbleibt, indem er nur mit dem Begriffe des quadratischen Restes selbst operiert; dabei ist seine Methode die der allgemeinen Induktion. Durch diese Methode, der sie gleichfalls folgen, treten dem genannten Gaufsischen Beweise diejenigen von Kronecker (23), Hermes (33) und Schmidt (41, Nr. 3) an die Seite; doch sind im übrigen ihre Wege wesentlich andere; enger oder loser schliefsen sie sich an diejenige Kategorie an, die wir als fünfte charakterisieren werden; ferner der von Bang (43).

Eine zweite Kategorie ist diejenige, in welcher die Beweise, wie der zweite Gaufsische und wie auch bereits Legendre's erwähnter Beweisversuch, auf die Theorie der quadratischen Formen begründet sind; hierin gehören noch die Beweise von Kummer (19).

Zur dritten Kategorie rechnen die Beweise 3 und 18, welche sich der Theorie der höheren Kongruenzen bedienen.

Die Beweise der vierten Kategorie gründen sich auf die

Lehre von der Kreisteilung; ihrer ist eine ziemliche Anzahl, die Beweise 5, 7, 8, 9, 10, 11, 13, 14, 15; am zahlreichsten aber ist die fünfte Kategorie, der wir die übrigen zuzählen, nämlich die Reihe derjenigen Beweise, welche das Gaufsische Lemma zum Ausgangspunkte nehmen oder doch wenigstens mit ihm sich verknüpfen.

In einer bereits erwähnten ausführlichen Abhandlung *„über das quadratische Reziprozitätsgesetz“*, die später auch als besondere Schrift (Leipzig, Teubner, 1885) erschienen ist, hat O. Baumgart sich der Aufgabe unterzogen, die Beweise dieses Gesetzes, soweit sie damals bekannt waren, darzustellen und in systematischem Zusammenhange zu beleuchten. Dieser interessante und wichtige Versuch, der auch uns mannigfachen Nutzen gewährt hat, bedarf, abgesehen von einigen Richtigstellungen, gegenwärtig, wo die Anzahl der Beweise sich noch beträchtlich gemehrt und die Einsicht vertieft hat, einer wesentlichen Ergänzung. Im Folgenden werden wir bemüht sein, nach Ausscheidung derjenigen Beweise, welche der zweiten, dritten und vierten Kategorie*) angehören und also nicht der „Niederen Zahlentheorie“ zugerechnet werden können, die gesamte Reihe der übrigen vergleichend darzustellen, indem wir sowohl ihre gemeinsamen Grundlagen, als ihre wesentlichen Unterschiede und damit ihr inneres Verhältnis zu einander in ein möglichst helles Licht zu setzen versuchen, dabei freilich davon absehen müssen, alle jene Beweise in ihren Einzelheiten zu reproduzieren; in dieser Hinsicht mufs auf die Originalarbeiten selbst verwiesen werden. —

9. Wir beginnen nun mit der Wiedergabe des ersten Gaufsischen Beweises. Die sehr umständliche Form desselben, bei welcher acht verschiedene Fälle einzeln zu behandeln waren, ist auf geistvolle Weise von Lejeune Dirichlet**) mit Hilfe des Legendreschen Symbols wesentlich vereinfacht und die acht Fälle auf zwei verschiedene zusammengezogen worden; wir schliefsen uns also des Letzteren Darstellung an.

Das Reziprozitätsgesetz, wie es die Formel (45) zum Ausdrucke bringt, besagt offenbar, dafs der quadratische Charakter einer ungeraden Primzahl q zu einer anderen ungeraden Primzahl p derselbe ist, wie derjenige von p zu q, in Zeichen: $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, wenn nicht beide Primzahlen von der Form $4z + 3$ sind; dafs aber im letzteren Falle der quadratische Charakter von q zu p der entgegengesetzte ist,

*) Bezüglich der Beweise der dritten Kategorie s. Kap. 7, Nr. 29.

**) Dirichlet, über den ersten der von Gaufs gegebenen Beweise des Reziprozitätsgesetzes, *J. f. Math.* 47, 1854, p. 139, oder auch: *Vorlesungen über Zahlentheorie*, herausg. von Dedekind, 4. Aufl., 1894, p. 112.

wie der von p zu q, in Zeichen: $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$. Ferner wissen wir, dafs, wenn dies richtig ist für alle Primzahlen unterhalb irgend einer gegebenen Grenze, auch das allgemeinere Reziprozitätsgesetz (56) statthat für alle relativ prime Zahlen P, Q, die nur aus solchen Primfaktoren zusammengesetzt und nicht beide negativ sind. Wir nehmen nun an, das Gesetz (45) gelte für je zwei ungerade Primzahlen, welche kleiner sind als die Primzahl q; beweisen wir dann, dafs es auch richtig ist für jede Kombination aus q und einer jeden jener Primzahlen, so gilt es allgemein, denn in der That besteht es für das Paar 3, 5, da die Zahl 3 (mod. 5) und wegen $5 \equiv 2$ (mod. 3) auch 5 (mod. 3) quadratischer Nichtrest, somit $\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right)$ ist.

Sei p irgend eine ungerade Primzahl $< q$. Entweder ist dann q von der Form $4z + 3$. Da -1 in Bezug auf eine solche Primzahl quadratischer Nichtrest ist, mufs $+p$ oder $-p$ quadratischer Rest (mod. q) sein; bei passender Wahl des Vorzeichens in der Formel $\pi = \pm p$ ist also

$$\left(\frac{\pi}{q}\right) = 1.$$

Diese Formel besteht im anderen Falle, wo q von der Form $4z + 1$ ist, sogar für beide Vorzeichen, falls p quadratischer Rest ist von q; dagegen für keins derselben, falls p quadratischer Nichtrest von q ist.

Demnach unterscheiden wir zwei Fälle:

1) im ersten bestehe für die Primzahlen p, q und eins der Vorzeichen in der Formel $\pi = \pm p$ die Gleichung

$$\left(\frac{\pi}{q}\right) = 1; \tag{61}$$

2) im zweiten sei q von der Form $4z + 1$ und $\left(\frac{p}{q}\right) = -1$.

Im erstgenannten Falle ist die Kongruenz $x^2 \equiv \pi$ (mod. q) möglich und hat zwei Wurzeln; wählt man diese positiv und kleiner als q, so ist eine von ihnen, da sie (mod. q) entgegengesetzt also von der Form ξ, $q - \xi$ sind, gerade; sie heifse e, sodafs

$$e^2 - \pi = q \cdot f \tag{62}$$

gesetzt werden kann, wo f, wie einfach zu erkennen, eine ungerade und wegen $p < q$ positive Zahl $< q$ sein mufs.

Ist nun zuerst f nicht teilbar durch π, so folgt aus (62)

$$\left(\frac{\pi}{f}\right) = 1, \quad \left(\frac{qf}{\pi}\right) = 1,$$

mithin, da für die beiden Zahlen π, f, welche $< q$, relativ prim und nicht beide negativ sind, das allgemeine Reziprozitätsgesetz angenommen werden darf,

$$(63)\qquad \left(\frac{q}{\pi}\right) = (-1)^{\frac{\pi-1}{2}\cdot\frac{f-1}{2}},$$

während ferner aus (62), da e gerade ist,

$$-\pi \equiv qf \pmod{4}$$

also

$$\left.\begin{aligned} -\frac{\pi+1}{2} &\equiv \frac{q-1}{2} + \frac{f-1}{2} \\ -\frac{\pi-1}{2}\cdot\frac{\pi+1}{2} &\equiv \frac{q-1}{2}\cdot\frac{\pi-1}{2} + \frac{\pi-1}{2}\cdot\frac{f-1}{2} \end{aligned}\right\} \pmod{2},$$

mithin, da das Produkt zweier successiver Zahlen gerade ist,

$$\frac{\pi-1}{2}\cdot\frac{f-1}{2} \equiv \frac{\pi-1}{2}\cdot\frac{q-1}{2} \pmod{2},$$

statt (63) also

$$(64)\qquad \left(\frac{q}{\pi}\right) = (-1)^{\frac{\pi-1}{2}\cdot\frac{q-1}{2}}$$

erschlossen wird, wie es der Formel (45) bezw. (56) gemäfs ist.

Wäre dagegen f teilbar durch π, $f = \pi f'$, so müfste wegen (62) auch e durch π teilbar sein, $e = \pi e'$, sodafs (62) übergeht in die Gleichung

$$(65)\qquad \pi e'^2 - 1 = qf'.$$

Aus der letztern aber folgt zunächst, dafs jetzt f' und π, ebenso wie f' und e' relative Primzahlen sind, ferner folgen die Gleichungen

$$\left(\frac{-qf'}{\pi}\right) = 1,$$

$$\left(\frac{\pi e'^2}{f'}\right) = \left(\frac{\pi}{f'}\right) = \left(\frac{\pi}{-f'}\right) = 1,$$

wo für die Zahlen π, $-f'$, welche nicht beide negativ, relativ prim und $< q$ sind, das allgemeine Reziprozitätsgesetz angenommen werden darf; aus ihrer Kombination ergiebt sich demnach die andere:

$$(66)\qquad \left(\frac{q}{\pi}\right) = (-1)^{\frac{\pi-1}{2}\cdot\frac{f'+1}{2}},$$

welche, da wegen (65)

$$-1 \equiv qf' \pmod{4} \quad \text{also} \quad \frac{f'+1}{2} \equiv \frac{q-1}{2} \pmod{2}$$

ist, wieder durch die Gleichung (64) ersetzt werden kann. Mithin besteht in dem ersten der beiden unterschiedenen Fälle das Reziprozitätsgesetz auch noch für die Kombination der beiden Primzahlen p, q, w. z. b. w.

Im zweitgenannten Falle bietet sich von vornherein nicht die Möglichkeit dar, eine Gleichung anzusetzen, wie die Gleichung (62),

aus der man weitere Folgerungen ableiten kann, man mufs daher darauf bedacht sein, zu einer solchen zu gelangen. Hierzu dient der Nachweis, dafs wenigstens eine Primzahl $p' < q$ vorhanden ist, für welche

(67) $$\left(\frac{q}{p'}\right) = -1,$$

oder dafs q nicht in Bezug auf alle Primzahlen $< q$ quadratischer Rest ist. Wir werden diesen Nachweis, welcher den eigentlichsten Grundstein des ersten Gaufsschen Beweises ausmacht, nachher erbringen; setzen wir eine solche Primzahl p' als vorhanden voraus, so folgt das Reziprozitätsgesetz aus ganz ähnlichen Schlüssen wie zuvor.

Zunächst leuchtet ein, dafs $\left(\frac{p'}{q}\right) = -1$ sein, für das Paar p', q also das Reziprozitätsgesetz Giltigkeit haben mufs; denn, wäre im Gegenteil $\left(\frac{p'}{q}\right) = +1$, so befänden wir uns im erstgenannten Falle und hätten folglich

$$\left(\frac{q}{p'}\right) = (-1)^{\frac{p'-1}{2}\cdot\frac{q-1}{2}} = +1$$

gegen die Voraussetzung. Zum Beweise des Reziprozitätsgesetzes bleibt also nur noch zu zeigen, dafs, wenn es noch eine von p' verschiedene Primzahl $p < q$ giebt, für welche $\left(\frac{p}{q}\right) = -1$ ist, auch $\left(\frac{q}{p}\right) = -1$, oder, was wegen (67) auf dasselbe hinauskommt, dafs

(68) $$\left(\frac{q}{pp'}\right) = 1$$

ist.

Da umgekehrt $\left(\frac{pp'}{q}\right) = 1$ also pp' quadratischer Rest von p ist, so erhält man eine Gleichung von der Form

(69) $$e^2 - pp' = qf,$$

in welcher $e < q$ eine gerade, f aber eine ungerade Zahl ist, die ebenfalls $< q$ sein mufs. Nun ist

entweder f relativ prim zu pp'; dann folgt aus (69) $\left(\frac{pp'}{f}\right) = 1$ und, da qf nach derselben Gleichung quadratischer Rest von pp' also $\left(\frac{qf}{pp'}\right) = 1$, auf die Zahlen f und pp' aber ersichtlich das allgemeine Reziprozitätsgesetz anwendbar ist, findet sich sogleich

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{f-1}{2}\cdot\frac{pp'-1}{2}},$$

während sich aus (69)

$$-pp' \equiv qf \pmod{4}$$

mithin

$$-\frac{pp'+1}{2} \equiv \frac{q-1}{2} + \frac{f-1}{2}, \quad \frac{f-1}{2} \cdot \frac{pp'-1}{2} \equiv \frac{q-1}{2} \cdot \frac{pp'-1}{2} \pmod{2}$$

und deshalb

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{q-1}{2} \cdot \frac{pp'-1}{2}} = 1$$

ergiebt.

Oder aber f ist durch p' teilbar, nicht teilbar durch p, d. i. $f = p'f'$, wo f' zu p prim ist. Dann mufs auch $e = p'e'$ sein und die Gleichung (69) nimmt die Gestalt an:

$$p'e'^2 - p = qf', \tag{70}$$

weshalb f' auch prim ist gegen p' und e', wie die letztere Zahl gegen p. Hieraus fliefsen die Gleichungen

$$\left(\frac{p'}{f'}\right) = \left(\frac{p}{f'}\right) \quad \text{oder} \quad \left(\frac{pp'}{f'}\right) = 1,$$

$$\left(\frac{qf'}{p}\right) = \left(\frac{p'}{p}\right), \quad \left(\frac{qf'}{p'}\right) = \left(\frac{-p}{p'}\right)$$

folglich

$$\left(\frac{q}{pp'}\right) \cdot \left(\frac{f'}{pp'}\right)\left(\frac{pp'}{f'}\right) = \left(\frac{p'}{p}\right) \cdot \left(\frac{-p}{p'}\right),$$

oder, da auf die Zahlen pp', f' das allgemeine Reziprozitätsgesetz angewandt werden darf, einfacher

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{f'-1}{2} \cdot \frac{pp'-1}{2} + \frac{p'-1}{2} \cdot \frac{p+1}{2}}.$$

Nun ist wegen (70)

$$-p \equiv qf' \pmod{4} \quad \text{also} \quad \frac{f'-1}{2} \equiv \frac{p+1}{2} \pmod{2},$$

der vorige Exponent ist daher (mod. 2) kongruent mit

$$\frac{p+1}{2}\left(\frac{pp'-1}{2} + \frac{p'-1}{2}\right) \equiv \frac{p+1}{2} \cdot \frac{p-1}{2} \equiv 0$$

und folglich $\left(\frac{q}{pp'}\right) = +1$.

Man bemerke, dafs bei diesem Räsonnement nirgends von der besonderen Beschaffenheit der Primzahl p', nach welcher $\left(\frac{q}{p'}\right) = -1$ sein soll, Gebrauch gemacht worden ist; da im übrigen die Rolle der Primzahlen p, p' genau die gleiche ist, so wird man durch das analoge Räsonnement zu eben demselben Schlusse kommen, wenn man umgekehrt f durch p teilbar, nicht teilbar durch p' voraussetzt.

Sei endlich noch f teilbar durch pp', $f = pp' \cdot f'$, also auch $e = pp' \cdot e'$ und demnach

$$pp' \cdot e'^2 - 1 = qf'. \tag{71}$$

Man schliefst zunächst $\left(\frac{pp'}{f'}\right) = 1$, $\left(\frac{-qf'}{pp'}\right) = 1$, also, da auf die Zahlen $pp', -f'$ das allgemeine Reziprozitätsgesetz anwendbar ist,

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{pp'-1}{2} \cdot \frac{f'+1}{2}}.$$

Da aber wegen (71)

$$-1 \equiv qf' \pmod{4}, \quad \text{also} \quad \frac{f'+1}{2} \equiv \frac{q-1}{2} \pmod{2}$$

d. i. gerade ist, so ergiebt sich auch jetzt wieder, was zu zeigen war,

$$\left(\frac{q}{pp'}\right) = 1. \text{ —}$$

Zur Giltigkeit des Reziprozitätsgesetzes ist jetzt nur noch die Lücke zu ergänzen, welche im Vorigen verblieb, nämlich das Vorhandensein einer ungeraden Primzahl $p' < q$ nachzuweisen, für welche $\left(\frac{q}{p'}\right) = -1$.

Dies ist sehr einfach, falls q von der Form $8z + 5$; denn alsdann ist $\frac{q+1}{2}$ von der Form $4z + 3$ und diese Zahl deshalb durch mindestens einen Primfaktor derselben Form teilbar, da Primfaktoren der Form $4z + 1$ allein auch nur Produkte dieser letzteren Form hervorbringen können. Ist also p' ein Primfaktor von $\frac{q+1}{2}$ von der Form $4z + 3$, so ist auch $q + 1$ durch p' teilbar also $q \equiv -1 \pmod{p'}$ und $\left(\frac{q}{p'}\right) = \left(\frac{-1}{p'}\right) = -1$.

Ist dagegen q von der Form $8z + 1$, so liegt die Sache viel schwieriger, und es bedurfte des angestrengtesten Nachdenkens, bis es Gaufs gelang, diesen Punkt durch einen Gedankengang festzustellen, der, wie Kronecker (*Berl. Monatsber.* 1876, p. 341) mit Recht gesagt hat, „als eine Kraftprobe Gaufsschen Geistes“ angesehen werden kann. Wäre nämlich in diesem Falle q quadratischer Rest von jeder Primzahl, welche eine ungerade Zahl $2m + 1 < q$ nicht übertrifft, so wäre q, da es von der Form $8z + 1$ also auch für jede Potenz von 2 quadratischer Rest ist, auch in Bezug auf jeden Modulus, der nur aus Zahlen $\overline{\gtrless}\, 2m + 1$ zusammengesetzt ist, quadratischer Rest, und demnach wäre, wenn

$$M = 1 \cdot 2 \cdot 3 \cdots 2m(2m+1)$$

gesetzt wird, die Kongruenz

$$x^2 \equiv q \pmod{M}$$

auflösbar. Sei $x = k$ eine ihrer Lösungen, dann ist k wie q relativ prim zu M und

$$\begin{aligned} k \cdot (q - 1^2)(q - 2^2) \cdots (q - m^2) &\equiv k(k^2 - 1^2)(k^2 - 2^2) \cdots (k^2 - m^2) \\ &\equiv (k+m)(k+m-1) \cdots (k+1)\, k\, (k-1) \cdots (k-m+1)(k-m) \end{aligned}$$

und folglich $\equiv 0 \pmod{M}$, da das Produkt der $2m + 1$ aufeinander-

folgenden Zahlen zur Rechten teilbar ist durch M (Kap. 2 Nr. 12); es würde daher der Quotient

$$\frac{1}{m+1} \cdot \frac{q-1^2}{(m+1)^2-1^2} \cdot \frac{q-2^2}{(m+1)^2-2^2} \cdots \frac{q-m^2}{(m+1)^2-m^2},$$

dessen Nenner mit M gleich ist, eine ganze Zahl sein. Wählt man indessen $m < \sqrt{q} < m+1$, was mit der Bedingung $2m+1 < q$ verträglich ist, da die kleinste Primzahl von der Form $8z+1$ die Zahl $q = 17$ ist, so ist ersichtlich jeder Faktor des obigen Ausdrucks ein echter Bruch. Demnach kann q nicht quadratischer Rest von jeder Primzahl $\overline{\gtrless}\, 2m+1$ also auch nicht von jeder Primzahl $< q$ sein, w. z. b. w. —

10. Wendet man sich nun dazu, die Reihe von Beweisen, welche das Gaufssche Lemma zur Grundlage nehmen, nach ihrem inneren Zusammenhange zu entwickeln, so wird man vor allem sich klar zu machen haben, welche Handhabe jenes Lemma zu dem gewollten Beweise darbietet.

Sind aber P, Q zwei positive, ungerade, relativ prime Zahlen, so besagt das verallgemeinerte Gaufssche Lemma, dafs

$$\left(\frac{Q}{P}\right) = (-1)^{\mu(Q,P)} \tag{72}$$

sei, wenn $\mu(Q, P)$ die Anzahl der negativen absolut kleinsten Reste in der Reihe

$$1 \cdot Q,\ 2 \cdot Q,\ 3 \cdot Q, \cdots P' \cdot Q \pmod{P} \tag{73}$$

bedeutet, in welcher P' zur Abkürzung für $\frac{P-1}{2}$ gesetzt ist. Desgleichen ist

$$\left(\frac{P}{Q}\right) = (-1)^{\mu(P,Q)}, \tag{74}$$

wenn $\mu(P, Q)$ die Anzahl der negativen absolut kleinsten Reste in der Reihe

$$1 \cdot P,\ 2 \cdot P,\ 3 \cdot P, \cdots Q' \cdot P \pmod{Q} \tag{75}$$

bezeichnet, wo Q' statt $\frac{Q-1}{2}$ gesetzt ist. Da aus (72) und (74) sich

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\mu(P,Q)+\mu(Q,P)} \tag{76}$$

ergiebt, so ist zum Beweise des Reziprozitätsgesetzes nur zu zeigen, dafs

$$\mu(P, Q) + \mu(Q, P) \equiv \frac{P-1}{2} \cdot \frac{Q-1}{2} \pmod{2} \tag{77}$$

ist.

In der besonderen Art und Weise, diesen Nachweis zu erbringen, unterscheiden sich nun jene Beweise voneinander und können nach

ihr gruppiert werden. So gehen die einen mehr darauf aus, einen der Teile $\mu(P, Q)$, $\mu(Q, P)$ für sich zu bestimmen, um dann ihn mit dem andern in Beziehung zu setzen, andere führen diese Teile auf andere Zahlen zurück, „welche die Eigenschaft der Reziprozität in einer leicht erkennbaren Form enthalten" (Schering, *Gött. Nachr.* 1879, p. 21), und bestimmen symmetrischer die Summe $\mu(P, Q) + \mu(Q, P)$ selbst. Dies und ähnliches sind aber mehr nur formelle als prinzipielle Unterschiede, welch' letztere vielmehr in der verschiedenen Quelle oder Grundlage zu suchen sein werden, welcher in den einzelnen Beweisen die Bestimmung der sogenannten „charakteristischen Zahlen" $\mu(P, Q)$, $\mu(Q, P)$ entnommen wird. In dieser Hinsicht wird man durch die Definition der Zahl $\mu(Q, P)$ wesentlich auf die Betrachtung der Bedingungen geführt, unter welchen in der Kongruenz

$$hQ \equiv \pm h' \pmod{P}, \tag{78}$$

wo sowohl h als h' eine der Zahlen $1, 2, 3, \cdots \frac{P-1}{2}$ bedeutet, oder auch in der gleichbedeutenden Gleichung

$$hQ - kP = \pm h' \tag{79}$$

das positive oder das negative Vorzeichen eintreten mufs, und in der verschiedenen Erfassung oder Ausbeutung der Verhältnisse, welche hierüber entscheiden, beruht die prinzipielle Verschiedenheit der einzelnen Beweise. Es ist wesentlich Kroneckers Verdienst, durch immer erneutes und tieferes Eindringen in jene Verhältnisse oder in die einfachsten Voraussetzungen, welche den verschiedenen Beweisen zu Grunde liegen, für die gröfsere Mehrheit derselben ihr inneres Verhältnis zu einander klargelegt (s. darüber namentlich seine Abhandlung „die absolut kleinsten Reste reeller Gröfsen", *Berl. Sitzungsber.* 1885, p. 383, 1045), und somit eine systematische Darstellung derselben, wie wir sie nun versuchen werden, ermöglicht zu haben; mehrere andere, namentlich neuere Beweise fügen sich dann in etwas loserem Zusammenhange ihnen an.

Hierbei macht man in vorteilhafter Weise von gewissen Bezeichnungen Gebrauch, welche gleich hier eingeführt werden sollen und gleichfalls Kronecker zu verdanken sind. Indem wir nach wie vor mit $[x]$ die gröfste ganze Zahl (nach Schering $\mathfrak{G}\mathfrak{G}(x)$) bezeichnen, welche in dem reellen Werte x enthalten, nämlich durch die Ungleichheiten

$$[x] \leqq x < [x] + 1 \tag{80}$$

definiert ist, nennen wir $g(x)$ (nach Schering $\mathfrak{N}\mathfrak{G}(x)$) die nächst an x gelegene ganze Zahl, von welcher sich daher x in plus oder minus um weniger als $\frac{1}{2}$ unterscheidet; wir definieren mithin

$$(81)\quad \begin{aligned} g(x) &= [x], \qquad \text{wenn}\quad [x] \overline{\overline{<}}\, x < [x] + \tfrac{1}{2},\\ g(x) &= [x]+1, \quad \text{wenn}\quad [x]+\tfrac{1}{2} \overline{\overline{<}}\, x < [x]+1; \end{aligned}$$

läge x gerade in der Mitte zwischen zwei ganzen Zahlen, sodafs $x = [x] + \frac{1}{2}$, so haben wir $g(x)$, da es seiner Bedeutung nach dann zweideutig würde, um es auch für diesen Fall zu fixieren, gleich $[x]+1$ gewählt. Man erkennt so unverzüglich, dafs immer

$$(82)\qquad g(x) = \left[x + \frac{1}{2}\right]$$

gesetzt werden darf.

Versteht man nun unter $R(x)$ den Unterschied

$$(83)\qquad R(x) = x - \left[x + \frac{1}{2}\right]$$

zwischen x und der nächstgelegenen ganzen Zahl, so ist dieser Unterschied stets absolut kleiner als $\frac{1}{2}$, zudem aber positiv resp. negativ, jenachdem

$$x - [x] < \frac{1}{2} \quad \text{oder} \quad x - [x] \overline{\overline{>}} \frac{1}{2}$$

ist.

Endlich wollen wir mit sgn. x die positive oder negative Einheit bezeichnen, jenachdem $x > 0$ oder $x < 0$ ist, sodafs auch

$$(84)\qquad \text{sgn.}\, x = \frac{x}{|x|}$$

gesetzt werden kann, wenn, wie üblich, durch $|x|$ der Absolutwert von x ausgedrückt wird. Für den singulären Wert $x = 0$ soll auch unter dem Zeichen sgn. x die Null verstanden werden. Dieser Definition zufolge besteht offenbar die Beziehung

$$(85)\qquad \text{sgn.}\, xy = \text{sgn.}\, x \cdot \text{sgn.}\, y,$$

von der sehr vielfacher Gebrauch gemacht werden wird. In Anwendung solcher Bezeichnungen dürfen wir dann für ein von Null verschiedenes x sagen:

es sei sgn. $R(x) = \pm 1$, jenachdem $x - [x] < \frac{1}{2}$ oder $\overline{\overline{>}} \frac{1}{2}$ ist.

Nun gilt in der Kongruenz (78) das obere oder das untere Vorzeichen, jenachdem der kleinste positive Rest von hQ (mod. P) kleiner oder gröfser ist als $\frac{P}{2}$, oder, was dasselbe sagt, jenachdem $\frac{hQ}{P} - \left[\frac{hQ}{P}\right] <$ oder $> \frac{1}{2}$, also

$$\text{sgn.}\, R\left(\frac{hQ}{P}\right) = +1 \text{ resp. } -1$$

ist. Da ferner das Letztere, wenn h die Werte $1, 2, 3, \cdots \frac{P-1}{2}$ durchläuft, $\mu(Q, P)$-mal geschieht, so wird

$$(86) \qquad \prod_{h=1}^{P'} \text{sgn.}\, R\left(\frac{hQ}{P}\right) = (-1)^{\mu(Q,P)}$$

und folglich nach dem Gaufsschen Lemma

$$(87) \qquad \left(\frac{Q}{P}\right) = \prod_{h=1}^{P'} \text{sgn.}\, R\left(\frac{hQ}{P}\right)$$

sein.

Auf gleiche Weise ergiebt sich

$$\left(\frac{P}{Q}\right) = \prod_{k=1}^{Q'} \text{sgn.}\, R\left(\frac{kP}{Q}\right);$$

demnach läfst sich das zu beweisende Reziprozitätsgesetz auch in folgender Formel aussprechen:

$$(88) \qquad \prod_{h=1}^{P'} \text{sgn.}\, R\left(\frac{hQ}{P}\right) \cdot \prod_{k=1}^{Q'} \text{sgn.}\, R\left(\frac{kP}{Q}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}$$

und besagt nichts anderes als den Satz: dafs unter den Werten

$$R\left(\frac{hQ}{P}\right) \quad \text{für} \quad h = 1, 2, 3, \cdots \frac{P-1}{2}$$

$$R\left(\frac{kP}{Q}\right) \quad \text{für} \quad k = 1, 2, 3, \cdots \frac{Q-1}{2}$$

die Anzahl $\mu(Q, P) + \mu(P, Q)$ derjenigen, welche negativ sind, nur dann ungerade sei, wenn P, Q beide von der Form $4z + 3$ sind, andernfalls immer gerade. Wir fügen sogleich noch einen dritten gleichbedeutenden Ausdruck des Gesetzes hier an. Offenbar ist

$$\frac{1}{2}(1 - \text{sgn.}\, x) = 0 \text{ oder } 1,$$

jenachdem sgn. $x = 1$ oder -1 ist. Demnach wird

$$(89) \qquad \sum_{h=1}^{P'} \frac{1}{2}\left(1 - \text{sgn.}\, R\left(\frac{hQ}{P}\right)\right) = \mu(Q, P)$$

und ebenso

$$\sum_{k=1}^{Q'} \frac{1}{2}\left(1 - \text{sgn.}\, R\left(\frac{kP}{Q}\right)\right) = \mu(P, Q);$$

die eben ausgesprochene Deutung des Reziprozitätsgesetzes findet daher ihren äquivalenten Ausdruck auch in der Kongruenz

$$(90)\qquad \sum_{h=1}^{P'} \tfrac{1}{2}\left(1-\text{sgn.}\,R\left(\tfrac{hQ}{P}\right)\right)+\sum_{k=1}^{Q'} \tfrac{1}{2}\left(1-\text{sgn.}\,R\left(\tfrac{kP}{Q}\right)\right)$$
$$\equiv \frac{P-1}{2}\cdot\frac{Q-1}{2} \pmod{2}.$$

Wir werden von all' diesen Formulierungen in der Folge Gebrauch zu machen haben.

11. Während die zunächst zu besprechenden Beweise des Reziprozitätsgesetzes darin übereinkommen, sich sämtlich auf die Eigenschaften der Funktion $R(x)$ zu gründen, unterscheiden sie sich von einander durch den Umfang, in welchem sie diese Eigenschaften in Anspruch nehmen. Die fundamentalste dieser letzteren ist die, dafs

$$(91)\qquad R(x+1)=R(x)$$

ist; in der That, da für jeden reellen, positiven oder negativen Wert von x

$$(92)\qquad [x+1]=[x]+1$$

und daher allgemeiner, wenn z eine beliebige ganze Zahl bedeutet,

$$(93)\qquad [x+z]=[x]+z$$

ist, so besteht auch die Gleichung

$$\left[x+\tfrac{1}{2}+1\right]=\left[x+\tfrac{1}{2}\right]+1$$

und folglich auch

$$(x+1)-\left[x+1+\tfrac{1}{2}\right]=x-\left[x+\tfrac{1}{2}\right]$$

d. i. die Gleichung (91).

Da ferner stets

$$(94)\qquad [-x]=-[x]-1$$

ist — eine Gleichung, aus welcher in Verbindung mit (93) für jede ganze Zahl z giltig die andere hervorgeht:

$$(95)\qquad [x]+[z-x]=z-1$$

— so folgt, wenn $x+\frac{1}{2}$ statt x und $z=1$ gesetzt wird, die Beziehung:

$$\left[-x+\tfrac{1}{2}\right]=-\left[x+\tfrac{1}{2}\right]$$

also

$$(96)\qquad R(x)+R(-x)=0.$$

Mit Benutzung dieser Bezeichnungen und der angeführten Eigenschaften der Funktion $R(x)$ stellt sich nun zunächst der fünfte

Gaufssche Beweis, von welchem wir unsern Ausgangspunkt nehmen, folgendermafsen dar:

Seien immer P, Q zwei positive ungerade relativ prime Zahlen, so betrachte man die Reihe der Zahlen:

$$1, 2, 3, \ldots \frac{PQ-1}{2} \tag{97}$$

und teile sie in acht Klassen nach folgendem Prinzip:

1) in die erste Klasse nehme man alle Zahlen g der Reihe, für welche

$$\text{sgn.}\, R\left(\frac{g}{P}\right) = 1, \qquad \text{sgn.}\, R\left(\frac{g}{Q}\right) = 1$$

ist; ihre Anzahl sei α;

2) in die zweite diejenigen, für welche

$$\text{sgn.}\, R\left(\frac{g}{P}\right) = 1, \qquad \text{sgn.}\, R\left(\frac{g}{Q}\right) = -1$$

ist, ihre Anzahl sei β;

3) für die Zahlen der dritten Klasse mit der Anzahl γ sei

$$\text{sgn.}\, R\left(\frac{g}{P}\right) = -1, \qquad \text{sgn.}\, R\left(\frac{g}{Q}\right) = 1;$$

4) für die der vierten Klasse mit der Anzahl δ sei

$$\text{sgn.}\, R\left(\frac{g}{P}\right) = -1, \qquad \text{sgn.}\, R\left(\frac{g}{Q}\right) = -1;$$

5) für die der fünften Klasse sei

$$\text{sgn.}\, R\left(\frac{g}{P}\right) = 0, \qquad \text{sgn.}\, R\left(\frac{g}{Q}\right) = 1;$$

6) für die der sechsten Klasse sei

$$\text{sgn.}\, R\left(\frac{g}{P}\right) = 0, \qquad \text{sgn.}\, R\left(\frac{g}{Q}\right) = -1;$$

die Zahlen dieser beiden Klassen zusammengenommen sind die Vielfachen

$$1 \cdot P, \quad 2 \cdot P, \quad 3 \cdot P, \ldots \frac{Q-1}{2} \cdot P$$

und folglich ist die Anzahl derjenigen der letzten Klasse $\mu(P, Q)$, somit die Anzahl derjenigen der vorletzten Klasse gleich $\frac{Q-1}{2} - \mu(P, Q)$;

7) für die siebente Klasse sei

$$\text{sgn.}\, R\left(\frac{g}{P}\right) = 1, \qquad \text{sgn.}\, R\left(\frac{g}{Q}\right) = 0;$$

8) für die achte Klasse endlich sei

$$\text{sgn.}\, R\left(\frac{g}{P}\right) = -1, \qquad \text{sgn.}\, R\left(\frac{g}{Q}\right) = 0;$$

die Anzahl der Zahlen in dieser und der voraufgehenden Klasse sind offenbar $\mu(Q, P)$ und $\frac{P-1}{2} - \mu(Q, P)$ resp.

Die Zahlen der vier ersten Klassen sind zusammen die weder durch P noch durch Q teilbaren Zahlen (97), ihre Anzahl also gleich $\frac{PQ-1}{2} - \frac{P-1}{2} - \frac{Q-1}{2}$, und somit besteht die Beziehung

$$\alpha + \beta + \gamma + \delta = \frac{(P-1)(Q-1)}{2}. \tag{98}$$

Betrachtet man aber die Summe

$$\sum_{g=1}^{\frac{PQ-1}{2}} \text{sgn.}\, R\left(\frac{g}{P}\right) \cdot \text{sgn.}\, R\left(\frac{g}{Q}\right), \tag{99}$$

welche mit Rücksicht auf die Eigenschaft (96) der Funktion $R(x)$ auch durch die folgende:

$$\frac{1}{2} \cdot \sum_{-\frac{PQ-1}{2}}^{\frac{PQ-1}{2}} \text{sgn.}\, R\left(\frac{g}{P}\right) \cdot \text{sgn.}\, R\left(\frac{g}{Q}\right)$$

ersetzt werden kann, welche auf ein vollständiges Restsystem (mod. PQ) erstreckt ist, so darf man hier wegen der fundamentalen Eigenschaft (91) der Funktion $R(x)$, der zufolge $R\left(\frac{g}{P}\right)$, $R\left(\frac{g}{Q}\right)$ sich nicht ändern, wenn g durch eine ihm (mod. PQ) kongruente Zahl ersetzt wird, statt dieses speziellen Restsystems auch ein anderes, z. B. dasjenige wählen, das aus den Zahlen $g = hQ + kP$ für $h = 0, \pm 1, \pm 2, \cdots \pm \frac{P-1}{2}$; $k = 0, \pm 1, \pm 2, \cdots \pm \frac{Q-1}{2}$ besteht; dann aber läſst sich die Summe als das Produkt zweier anderen schreiben, wie folgt:

$$\frac{1}{2} \cdot \sum_{h=0, \pm 1, \pm 2, \cdots \pm P'} \text{sgn.}\, R\left(\frac{hQ}{P}\right) \cdot \sum_{k=0, \pm 1, \pm 2, \cdots \pm Q'} \text{sgn.}\, R\left(\frac{kP}{Q}\right),$$

deren jede aber wegen (96) den Wert Null hat. Demnach ist auch die Summe (99) gleich Null. Denkt man jedoch in ihr die Zahlen g in die angegebenen acht Klassen zerlegt, so leuchtet ein, daſs sie mit dem Ausdrucke

$$\alpha - \beta - \gamma + \delta$$

identisch ist, und man gewinnt zwischen den Anzahlen $\alpha, \beta, \gamma, \delta$ die zweite Beziehung

$$\alpha - \beta - \gamma + \delta = 0, \tag{100}$$

aus deren Verbindung mit der ersten (98) sich noch ferner:

$$(101) \qquad \alpha + \delta = \beta + \gamma = \frac{P-1}{2} \cdot \frac{Q-1}{2}$$

ergiebt.

Wir betrachten weiter die Summe

$$(102) \qquad \sum_{g=1}^{\frac{PQ-1}{2}} \operatorname{sgn.} R\left(\frac{g}{P}\right).$$

Für die ersten $\frac{P-1}{2}$ Werte von g ist $\frac{g}{P} < \frac{1}{2}$, mithin $\operatorname{sgn.} R\left(\frac{g}{P}\right) = 1$; von den nun folgenden können immer zwei von einander verschiedene: $\frac{P+1}{2} + r$ und $\frac{PQ-1}{2} - r$, zusammengefaſst werden; diese Zahlen können in der That einander nur gleich sein für den einzigen Wert $2r + 1 = \frac{P(Q-1)}{2}$, was voraussetzt, daſs Q von der Form $4z + 3$, also $\frac{Q+1}{4}$ ganzzahlig ist; für diesen Wert von r wäre aber

$$g = \frac{P+1}{2} + r = P \cdot \frac{Q+1}{4}$$

ein Vielfaches von P und das entsprechende Glied der Summe verschwände für sich; im übrigen aber verschwindet stets die Summe der gedachten zwei Glieder, da

$$R\left(\frac{P+1+2r}{2P}\right) + R\left(\frac{PQ-1-2r}{2P}\right) = R\left(\frac{1}{2} + \frac{1+2r}{2P}\right) + R\left(-\frac{1}{2} - \frac{1+2r}{2P}\right)$$

gesetzt werden kann, nach (96) also gleich Null ist. Somit findet sich

$$(103) \qquad \sum_{g=1}^{\frac{PQ-1}{2}} \operatorname{sgn.} R\left(\frac{g}{P}\right) = \frac{P-1}{2}$$

und auf gleiche Weise

$$\sum_{g=1}^{\frac{PQ-1}{2}} \operatorname{sgn.} R\left(\frac{g}{Q}\right) = \frac{Q-1}{2}.$$

Unterscheidet man nun in der letztern Summe die g nach den verschiedenen Klassen, in die wir sie verteilt haben, so verschwinden die Glieder der Summe, welche den beiden letzten Klassen entsprechen, und nach der angegebenen Anzahl der in den einzelnen übrigen Klassen enthaltenen Zahlen giebt die letzte Formel folgende neue Beziehung:

$$\left(\frac{Q-1}{2} - \mu(P, Q)\right) - \mu(P, Q) + \alpha - \beta + \gamma - \delta = \frac{Q-1}{2}$$

d. h.

$$2 \cdot \mu(P, Q) = \alpha - \beta + \gamma - \delta$$

oder wegen (98)

$$\mu(P, Q) + \beta + \delta = \frac{P-1}{2} \cdot \frac{Q-1}{2}, \tag{104}$$

der sich aus ähnlicher Betrachtung der Gleichung (103) die andere:

$$\mu(Q, P) + \gamma + \delta = \frac{P-1}{2} \cdot \frac{Q-1}{2} \tag{105}$$

an die Seite stellen läfst. Durch eine einfache Kombination der gefundenen Beziehungen aber erschliefst man nunmehr die nachstehenden vier Gleichungen:

$$\begin{aligned}
2\alpha &= \frac{P-1}{2} \cdot \frac{Q-1}{2} + \mu(P, Q) + \mu(Q, P),\\
2\beta &= \frac{P-1}{2} \cdot \frac{Q-1}{2} - \mu(P, Q) + \mu(Q, P),\\
2\gamma &= \frac{P-1}{2} \cdot \frac{Q-1}{2} + \mu(P, Q) - \mu(Q, P),\\
2\delta &= \frac{P-1}{2} \cdot \frac{Q-1}{2} - \mu(P, Q) - \mu(Q, P),
\end{aligned} \tag{106}$$

denen man noch die anderen hinzufügen kann:

$$\begin{aligned}
\mu(Q, P) &= \alpha - \gamma = \beta - \delta,\\
\mu(P, Q) &= \alpha - \beta = \gamma - \delta.
\end{aligned} \tag{107}$$

Unmittelbar aber giebt jede der Gleichungen (106), als Kongruenz (mod. 2) genommen, die Beziehung

$$\mu(P, Q) + \mu(Q, P) \equiv \frac{P-1}{2} \cdot \frac{Q-1}{2} \pmod{2}$$

d. i. die Kongruenz (77), welche das Reziprozitätsgesetz ausspricht (s. hierzu Kronecker, *Berl. Sitzgsber.* 1885, p. 383). —

12. Bevor nun der dritte Gaufsische Beweis angeschlossen werde, mufs eine fernere einfache Eigenschaft der Funktion $R(x)$ vorangestellt werden.

Jenachdem $R(x) > 0$ oder < 0 d. h. jenachdem in der Gleichung

$$x = [x] + \varrho$$

der Rest $\varrho < \frac{1}{2}$ oder $\gtreqless \frac{1}{2}$ ist, findet man aus

$$2x = 2[x] + 2\varrho$$

offenbar

$$[2x] - 2[x] = 0 \quad \text{oder} \quad 1.$$

Demnach ist für jedes nicht ganzzahlige x

$$\text{sgn.}\, R(x) = (-1)^{[2x]-2[x]} = (-1)^{[2x]}, \tag{108}$$

eine Formel, welcher auch wegen (95), so oft z eine ungerade Zahl ist, der Ausdruck

(109) $$\text{sgn.}\, R(x) = (-1)^{[z-2x]}$$

gegeben werden kann.

Hieraus ergiebt sich, wenn wieder P, Q zwei positive, ungerade, relativ prime Zahlen und h jede der Zahlen $1, 2, 3, \cdots \frac{P-1}{2}$ bedeutet,

(110) $$\text{sgn.}\, R\left(\frac{hQ}{P}\right) = (-1)^{\left[\frac{2hQ}{P}\right]} = (-1)^{\left[\frac{(P-2h)Q}{P}\right]}$$

und folglich nach (87)

(111) $$\left(\frac{Q}{P}\right) = (-1)^{\sum\limits_{h=1}^{P'}\left[\frac{2hQ}{P}\right]}$$

oder auch

(112) $$\left(\frac{Q}{P}\right) = (-1)^{\sum\limits_{h=1}^{P'}\left[\frac{(2h-1)Q}{P}\right]}.$$

Diesen beiden Formeln aber läfst sich noch eine dritte an die Seite stellen. Da man nämlich, wie Formel (110) aussagt, nach Belieben

$$\text{sgn.}\, R\left(\frac{hQ}{P}\right) = (-1)^{\left[\frac{2hQ}{P}\right]}$$

oder

$$\text{sgn.}\, R\left(\frac{hQ}{P}\right) = (-1)^{\left[\frac{(P-2h)Q}{P}\right]}$$

setzen kann, so darf man, wenn h die Reihe $1, 2, 3, \cdots \frac{P-1}{2}$ durchläuft, solange $h < \frac{P}{4}$ ist, die erste Formel wählen, wo dann $2h$ jede gerade Zahl $< \frac{P}{2}$ ist, wenn aber $h > \frac{P}{4}$ also $2h > \frac{P}{2}$ wird, die zweite Formel, in welcher dann $P - 2h$ jede ungerade Zahl $< \frac{P}{2}$ ist. Hierbei werden also die gedachten geraden und ungeraden Zahlen zusammen die ganze Reihe $1, 2, 3, \cdots \frac{P-1}{2}$ erfüllen, und man erhält das gesamte Produkt

$$\prod_{h=1}^{\frac{P-1}{2}} \text{sgn.}\, R\left(\frac{hQ}{P}\right) = (-1)^{\sum\limits_{h=1}^{\frac{P-1}{2}}\left[\frac{hQ}{P}\right]}$$

d. i. die Formel

(113) $$\left(\frac{Q}{P}\right) = (-1)^{\sum\limits_{h=1}^{\frac{P-1}{2}}\left[\frac{hQ}{P}\right]}.$$

Dieser Formel und dem verallgemeinerten Gaufsschen Lemma gemäfs wird also

$$(114)\qquad \mu(Q,P) \equiv \sum_{h=1}^{\frac{P-1}{2}} \left[\frac{hQ}{P}\right] \pmod{2}.$$

Der dritte **Gaufsische** Beweis stützt sich nun auf die letztere Kongruenz und besteht wesentlich in der Anwendung einer allgemeinen Formel zur Umformung der darin auftretenden Summe. Die gemeinte Formel ist die folgende: für positive Werte von x, für welche $x, 2x, 3x, \ldots nx$ gebrochene Werte sind, sodafs, wenn $[nx]=m$ gesetzt wird, $\frac{1}{x}, \frac{2}{x}, \frac{3}{x}, \cdots \frac{m}{x}$ ebenfalls solche Werte sind, besteht die Beziehung:

$$(115)\qquad \sum_{h=1}^{n} [hx] = mn - \sum_{k=1}^{m} \left[\frac{k}{x}\right].$$

An späterer Stelle gedenken wir auf diese und ähnliche Transformationsformeln zurückzukommen. Statt sie hier zu beweisen und dann auf die in (114) enthaltene Summe anzuwenden, ist es vorzuziehen, unmittelbar auf die letztere die Methode in Anwendung zu bringen, durch welche jene gewonnen wird. Wir setzen dabei der Klarheit wegen $P > Q$ voraus. Das erste Glied der Summe $\sum_{h=1}^{\frac{P-1}{2}} \left[\frac{hQ}{P}\right]$ hat den Wert $\left[\frac{Q}{P}\right] = 0$, das letzte den Wert

$$\left[\frac{(P-1)Q}{2P}\right] = \frac{Q-1}{2} < \frac{P-1}{2};$$

wir wollen immer diejenigen Glieder vereinigen, welche gleichen Wert haben. Sei dazu $\left[\frac{mQ}{P}\right]$ das letzte, welches den Wert $n-1$ hat, sodafs $\left[\frac{(m+1)Q}{P}\right] = n$ ist, und sei dann $\left[\frac{(m+m')Q}{P}\right]$ das letzte mit dem Werte n. Aus

$$\frac{mQ}{P} < n < \frac{(m+1)Q}{P}$$

folgt $m = \left[\frac{nP}{Q}\right]$, und auf dieselbe Weise $m + m' = \left[\frac{(n+1)P}{Q}\right]$, und folglich ist die Anzahl m' derjenigen Glieder der Summe, welche den Wert n haben,

$$m' = \left[\frac{(n+1)P}{Q}\right] - \left[\frac{nP}{Q}\right]$$

$$\text{für}\quad n = 1, 2, \cdots \frac{Q-3}{2};$$

für $n = \frac{Q-1}{2}$ dagegen findet sich die entsprechende Anzahl, da das letzte dieser Glieder das $\frac{P-1}{2}^{\text{te}}$ Glied der Summe ist, gleich

$$\frac{P-1}{2} - \left[\frac{Q-1}{2} \cdot \frac{P}{Q}\right].$$

Demnach erhält man

$$\sum_{h=1}^{\frac{P-1}{2}} \left[\frac{hQ}{P}\right] = 1 \cdot \left(\left[\frac{2P}{Q}\right] - \left[\frac{P}{Q}\right]\right) + 2 \cdot \left(\left[\frac{3P}{Q}\right] - \left[\frac{2P}{Q}\right]\right) + 3 \cdot \left(\left[\frac{4P}{Q}\right] - \left[\frac{3P}{Q}\right]\right)$$
$$\cdots + \frac{Q-3}{2} \cdot \left(\left[\frac{Q-1}{2} \cdot \frac{P}{Q}\right] - \left[\frac{Q-3}{2} \cdot \frac{P}{Q}\right]\right) + \frac{Q-1}{2} \cdot \left(\frac{P-1}{2} - \left[\frac{Q-1}{2} \cdot \frac{P}{Q}\right]\right)$$
$$= - \sum_{k=1}^{\frac{Q-1}{2}} \left[\frac{kP}{Q}\right] + \frac{Q-1}{2} \cdot \frac{P-1}{2}$$

oder die Gleichung

$$(116) \qquad \sum_{h=1}^{\frac{P-1}{2}} \left[\frac{hQ}{P}\right] + \sum_{k=1}^{\frac{Q-1}{2}} \left[\frac{kP}{Q}\right] = \frac{P-1}{2} \cdot \frac{Q-1}{2},$$

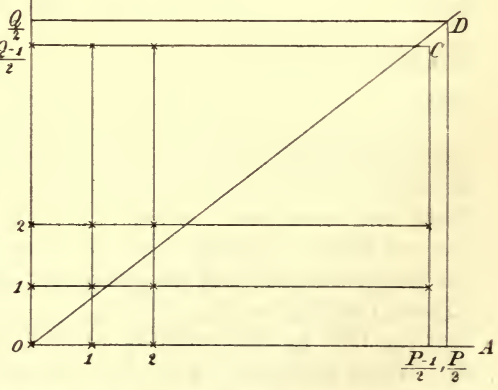
welche in der That aus (115) hervorgeht, wenn dort $x = \frac{Q}{P}$ und $n = \frac{P-1}{2}$ gesetzt wird, da alsdann $m = [nx] = \left[\frac{P-1}{2} \cdot \frac{Q}{P}\right] = \frac{Q-1}{2}$ wird. Mit Rücksicht auf die Kongruenz (114) und die ihr analoge:

$$\mu(P, Q) \equiv \sum_{k=1}^{\frac{Q-1}{2}} \left[\frac{kP}{Q}\right] \pmod{2}$$

geht aber aus der Gleichung (116) die Kongruenz

$$\mu(P, Q) + \mu(Q, P) \equiv \frac{P-1}{2} \cdot \frac{Q-1}{2} \pmod{2}$$

d. h. das verallgemeinerte Reziprozitätsgesetz hervor. —



Was in diesem Beweise durch die Transformation der Summe $\sum_{h=1}^{\frac{P-1}{2}} \left[\frac{hQ}{P}\right]$ erreicht wird, das liefert unmittelbar auf anschaulichem Wege Eisenstein's geometrischer Beweis (*J. f. Math.* 28, 1844, p. 246). Sei OA, OB

ein rechtwinkliges Axensystem, auf welchem die Strecken $\frac{P}{2}$, $\frac{Q}{2}$ resp. abgetragen sind; auf letzteren konstruiere man die Punkte $1, 2, 3, \cdots \frac{P-1}{2}$ resp. $1, 2, 3, \cdots \frac{Q-1}{2}$ und ziehe die Parallelen zu den Axen, deren in der Figur durch Sternchen gezeichnete Durchschnittspunkte „Netzpunkte“ heifsen mögen. Zieht man nun die Gerade OD mit der Gleichung

$$y = \frac{Q}{P}x \quad \text{oder} \quad x = \frac{P}{Q}y,$$

so ist augenscheinlich

$$\sum_{h=1}^{\frac{P-1}{2}} \left[\frac{hQ}{P}\right]$$

die Anzahl der Netzpunkte, welche im Rechtecke mit den Ecken $O, \frac{P-1}{2}, C, \frac{Q-1}{2}$ unterhalb, ebenso

$$\sum_{k=1}^{\frac{Q-1}{2}} \left[\frac{kP}{Q}\right]$$

die Anzahl der Netzpunkte, welche darin oberhalb OD liegen. Die Gesamtheit aller Netzpunkte in jenem Rechtecke beträgt aber $\frac{P-1}{2} \cdot \frac{Q-1}{2}$, mithin ergiebt sich die Gleichung (116) und damit wieder das Reziprozitätsgesetz. —

Achtet man genau auf das Prinzip der Umformung, der wir die Summe in (114) unterworfen haben, so sieht man der Reihe der Vielfachen

$$(117) \qquad 1 \cdot Q, \ 2 \cdot Q, \ 3 \cdot Q, \cdots \frac{P-1}{2} \cdot Q$$

diejenige der Vielfachen

$$(118) \qquad 1 \cdot P, \ 2 \cdot P, \ 3 \cdot P, \cdots \frac{Q-1}{2} \cdot P$$

gegenübergestellt und die erstere in Gruppen geteilt, deren Glieder zwischen je zwei aufeinanderfolgende Glieder der letzteren fallen. Statt nun zuerst die Formel (113) oder (114) herzuleiten und durch die auf dieser Gegenüberstellung beruhende Transformation derselben zur Reziprozitätsformel zu gelangen, kann man die letztere, wie Voigt (*Ztschr. für Math. u. Phys.* 26, 1881, p. 134) und J. C. Fields (*Amer. J.* 13, 1891, p. 189) im Wesentlichen übereinstimmend gezeigt haben, auch in der Weise gewinnen, dafs man unmittelbar ermittelt, wieviel Glieder in jeder jener Gruppen von Vielfachen (117), durch P geteilt, einen absolut kleinsten negativen, oder, was dasselbe sagt, einen kleinsten

positiven Rest $> \frac{P}{2}$ ergeben; im weiteren kommen dann übrigens nur Eigenschaften der Funktion $[x]$ oder $R(x)$, wie beim fünften Gaufsschen Beweise, in Betracht.

Zwischen die Vielfachen kP und $(k+1)P$ fallen die Vielfachen

$$(h+1)Q, \quad (h+2)Q, \cdots (h+h')Q,$$

wenn $hQ < kP < (h+1)Q$ und $(h+h')Q < (k+1)P < (h+h'+1)Q$ d. h.

$$h = \left[\frac{kP}{Q}\right], \qquad h + h' = \left[\frac{(k+1)P}{Q}\right]$$

gedacht wird; der kleinste positive Rest eines jener Vielfachen $(h+i)Q$ (mod. P) ist aber $> \frac{P}{2}$, wenn

$$(h+i)Q - kP > \frac{P}{2}$$

d. i. $i > (2k+1)\frac{P}{2Q} - \left[\frac{kP}{Q}\right]$ ist. Die Anzahl derartiger Vielfachen zwischen kP und $(k+1)P$ beträgt also, da

$$h' = \left[\frac{(k+1)P}{Q}\right] - \left[\frac{kP}{Q}\right]$$

die gesamte Anzahl der Vielfachen zwischen diesen Grenzen ist,

$$\left[\frac{(k+1)P}{Q}\right] - \left[\frac{(2k+1)P}{2Q}\right].$$

Dies gilt, wenn wieder, wie zuvor, $P > Q$ vorausgesetzt wird, sodafs $\frac{P-1}{2} \cdot Q > \frac{Q-1}{2} \cdot P$ ist, für $k = 0, 1, 2, \cdots \frac{Q-3}{2}$; dann liegen freilich auch noch einige Vielfache der Reihe (117) zwischen $\frac{Q-1}{2} \cdot P$ und $\frac{P-1}{2} \cdot Q$; da aber der Unterschied dieser Grenzen gleich $\frac{P-Q}{2}$ also $< \frac{P}{2}$ ist, so kann auch der Rest eines jeden der gedachten Vielfachen (mod. P) nur $< \frac{P}{2}$ sein, diesem letzten Intervalle entsprechen also keine Vielfachen der Reihe (117), wie sie hier in Frage kommen. Hieraus folgt, dafs die Gesamtzahl aller derartiger Vielfachen in der Reihe (117) d. h. die charakteristische Zahl $\mu(Q, P)$ gleich der Summe

$$\sum_{k=0}^{\frac{Q-3}{2}} \left(\left[\frac{(k+1)P}{Q}\right] - \left[\frac{(2k+1)P}{2Q}\right]\right)$$

oder auch

$$\mu(Q, P) = \sum_{k=1}^{\frac{Q-1}{2}} \left(\left[\frac{kP}{Q}\right] - \left[\frac{(2k-1)P}{2Q}\right]\right)$$

d. i., da man $2k-1$ bei der Summation auch durch $Q-2k$ ersetzen darf,

$$\mu(Q, P) = \sum_{k=1}^{\frac{Q-1}{2}} \left(\left[\frac{kP}{Q}\right] - \left[\frac{P}{2} - \frac{kP}{Q}\right] \right),$$

oder, wenn diese Gleichung als Kongruenz (mod. 2) aufgefafst wird,

$$\mu(Q, P) \equiv \sum_{k=1}^{\frac{Q-1}{2}} \left(\left[\frac{kP}{Q}\right] + \left[\frac{P}{2} - \frac{kP}{Q}\right] \right) \pmod{2}.$$

Aber wegen (93) ist

$$\left[\frac{P}{2} - \frac{kP}{Q}\right] = \frac{P-1}{2} + \left[\frac{1}{2} - \frac{kP}{Q}\right]$$

folglich

$$\mu(Q, P) \equiv \frac{P-1}{2} \cdot \frac{Q-1}{2} + \sum_{k=1}^{\frac{Q-1}{2}} \left(\left[\frac{kP}{Q}\right] + \left[\frac{1}{2} - \frac{kP}{Q}\right] \right),$$

wo nun das allgemeine Glied der Summe gleich 0 oder -1 ist, jenachdem der Rest von $\frac{kP}{Q}$ kleiner oder gröfser als $\frac{1}{2}$, d. h. jenachdem der Rest von kP (mod. Q) kleiner oder gröfser als $\frac{Q}{2}$ ist; die Summe reduziert sich also, da der letztere Fall in der Reihe (118) so oft eintritt, als die charakteristische Zahl $\mu(P, Q)$ angiebt, auf $-\mu(P, Q)$ und man erhält so die zu erweisende Beziehung:

$$\mu(Q, P) + \mu(P, Q) \equiv \frac{P-1}{2} \cdot \frac{Q-1}{2} \pmod{2}. \tag{119}$$

Anmerkung. Wenn man bei dieser Betrachtung die bisher als teilerfremd vorausgesetzten Zahlen P, Q im Gegenteil als mit einem gröfsten gemeinsamen Teiler d behaftet denkt, sodafs $P = dP_1$, $Q = dQ_1$ gesetzt werden kann, so mufs man bedenken, dafs dann bei der Zählung der Vielfachen hQ, deren Reste $> \frac{P}{2}$ (mod. P) sind, auch solche mit einbegriffen werden, welche Vielfache von P sind, deren Rest also in Wahrheit Null ist; dies sind die Vielfachen hQ, bei denen $h = iP_1$, $i < \frac{d}{2}$ ist, ihre Anzahl also gleich $\frac{d-1}{2}$. Will man mithin dem Zeichen $\mu(Q, P)$ die frühere Bedeutung wahren, so mufs man in der voraufgehenden Betrachtung dann $\mu(Q, P)$ durch $\mu(Q, P) + \frac{d-1}{2}$ ersetzen, während bei der Berechnung der letzten Summe diejenigen Vielfachen kP, welche Vielfache von Q sind, ein Glied Null geben, die Bedeutung von $\mu(P, Q)$ also die frühere bleibt.

Demnach verwandelt sich für diesen allgemeineren Fall die Kongruenz (119) in die folgende:

$$(120)\qquad \mu(P, Q) + \mu(Q, P) \equiv \frac{P-1}{2} \cdot \frac{Q-1}{2} + \frac{d-1}{2} \pmod{2}.$$

13. Noch mehrere andere Beweise sind, wie die letztbetrachteten, nur als eine Umformung des dritten Gaufsschen anzusehen, stehen demselben aber noch näher, insofern sie, wie in der Formel (108) oder (109) er selbst, von einem algebraischen Ausdrucke für $\operatorname{sgn.} R\left(\frac{hQ}{P}\right)$ ausgehen. Wir schicken ihnen eine einleitende Betrachtung voraus.

Die Kongruenz $hQ \equiv \varepsilon h' \pmod{P}$, in welcher $\varepsilon = \pm 1$, h und h' aber Zahlen der Reihe $1, 2, 3, \cdots \frac{P-1}{2}$ bedeuten, lautet, als Gleichung geschrieben, wie folgt:

$$hQ = \varepsilon h' + kP,$$

wo k eine ganze Zahl ist, und diese Gleichung ergiebt, wenn unter ω ein beliebiger reeller Wert verstanden wird, die andere:

$$\frac{hQ}{P}\omega = \frac{\varepsilon h'}{P}\omega + k\omega.$$

Ist demnach $\mathfrak{P}(x)$ irgend eine periodische Funktion mit der Periode ω, sodafs

$$(121)\qquad \mathfrak{P}(x+\omega) = \mathfrak{P}(x),$$

und besteht zudem die Beziehung

$$(122)\qquad \mathfrak{P}(x) + \mathfrak{P}(-x) = 0,$$

so erhält man unmittelbar die Beziehung

$$\mathfrak{P}\left(\frac{hQ}{P}\omega\right) = \varepsilon \cdot \mathfrak{P}\left(\frac{h'\omega}{P}\right)$$

oder

$$(123)\qquad \varepsilon = \frac{\mathfrak{P}\left(\frac{hQ\omega}{P}\right)}{\mathfrak{P}\left(\frac{h'\omega}{P}\right)}.$$

Den Gleichungen (91) und (96) zufolge ist $R(x)$ eine periodische Funktion der gedachten Art und ihre Periode $\omega = 1$; dasselbe gilt von $\operatorname{sgn.} R(x)$, da aus jenen Gleichungen offenbar auch diese:

$$\operatorname{sgn.} R(x+1) = \operatorname{sgn.} R(x)$$
$$\operatorname{sgn.} R(x) + \operatorname{sgn.} R(-x) = 0$$

hervorgehen. Wählt man also $\mathfrak{P}(x) = \operatorname{sgn.} R(x)$ und bedenkt, dafs $\frac{h'\omega}{P} = \frac{h'}{P} < \frac{1}{2}$, also $\operatorname{sgn.} R\left(\frac{h'\omega}{P}\right) = 1$ ist, so folgt aus (123)

$$\varepsilon = \operatorname{sgn.} R\left(\frac{hQ}{P}\right)$$

d. i. die frühere Bestimmungsweise von ε.

Statt dessen wählte **Eisenstein** (*J. f. Math.* 29, 1845, p. 177) $\mathfrak{P}(x) = \sin x$ also $\omega = 2\pi$, sodafs

$$\varepsilon = \text{sgn. } R\left(\frac{hQ}{P}\right) = \frac{\sin\frac{2hQ\pi}{P}}{\sin\frac{2h'\pi}{P}}$$

wurde, und erhielt mittels der Bemerkung, dafs h, h' gleichzeitig, wenn auch in anderer Anordnung, die Reihe $1, 2, 3, \cdots \frac{P-1}{2}$ durchlaufen, gemäfs (87) die Formel:

$$\left(\frac{Q}{P}\right) = \prod_{h=1}^{\frac{P-1}{2}} \frac{\sin\frac{2hQ\pi}{P}}{\sin\frac{2h\pi}{P}}.$$

Indem er nun auf diese Formel die Darstellung der Funktion $\frac{\sin Qx}{\sin x}$ als eine ganze Funktion von $\sin x$ und deren Zerlegung in Linearfaktoren zur Anwendung brachte, gab er dem Zeichen $\left(\frac{Q}{P}\right)$ einen Ausdruck, dessen Vergleichung mit dem entsprechenden Ausdrucke für $\left(\frac{P}{Q}\right)$ sofort das Reziprozitätsgesetz erkennen liefs. Ähnlich verfuhr **Liouville** (*Journ. de Math.* 12, p. 95; vgl. **Bachmann**, *Kreisteilung*, p. 118 ff.). Aus des Letztern Formeln erschlofs dann **Genocchi** (*Ac. R. Belgique, mém. couronnés* 25, 1853 (1852), *note sur la théorie des résidus quadratiques*, Chap. 13) eine Formel, aus welcher durch Spezialisierung

$$(124)\quad \frac{\sin\frac{2hQ\pi}{P}}{\sin\frac{2h\pi}{P}} = 2^{Q-1}\cdot(-1)^{\frac{Q-1}{2}}\cdot\prod_{k=1}^{\frac{Q-1}{2}} \sin\frac{2\pi(hQ+kP)}{PQ}\cdot\sin\frac{2\pi(hQ-kP)}{PQ}$$

hervorgeht. Beachtet man hier, dafs, wenn h eine der Zahlen $1, 2, 3, \cdots \frac{P-1}{2}$ und k eine der Zahlen $1, 2, 3, \cdots \frac{Q-1}{2}$ ist, $\frac{hQ+kP}{PQ}$ positiv und kleiner als 1, $\frac{hQ-kP}{PQ}$ aber zwischen $-\frac{1}{2}$ und $+\frac{1}{2}$ gelegen ist, und bedenkt, dafs deshalb nach den bekannten Eigenschaften der Sinusfunktion $\sin\frac{2\pi(hQ+kQ)}{PQ}$, $\sin\frac{2\pi(hQ-kP)}{PQ}$ nur dann negativ sind, wenn $\frac{hQ+kP}{PQ} > \frac{1}{2}$, resp. wenn $\frac{hQ-kP}{PQ} < 0$ ist; beachtet man weiter, dafs $\sin\frac{2h\pi}{P} > 0$, $\sin\frac{2hQ\pi}{P}$ aber positiv oder negativ ist, jenachdem der Rest von $\frac{hQ}{P} <$ oder $> \frac{1}{2}$, jenachdem

also sgn. $R\left(\frac{hQ}{P}\right)$ gleich $+1$ oder gleich -1 ist, so liest man aus der Gleichung (124) ohne weiteres die folgende ab:

$$(125)\qquad \text{sgn. } R\left(\frac{hQ}{P}\right) = (-1)^{\frac{Q-1}{2} + Ap_k\cdot\left(\frac{hQ+kP}{PQ}-\frac{1}{2}\right) + Ap_k\cdot\left(\frac{-hQ+kP}{PQ}\right)},$$

in welcher wir, im Anschlufs an eine Bezeichnungsweise, deren sich Schering in seinen bezüglichen Arbeiten bedient, unter den Zeichen

$$Ap_k\cdot\left(\frac{hQ+kP}{PQ}-\frac{1}{2}\right),\qquad Ap_k\cdot\left(\frac{-hQ+kP}{PQ}\right)$$

die Anzahl verstanden haben, wie oft die in Klammern stehenden Ausdrücke für die in Frage kommenden Werte von k, d. i. hier für die Werte $k = 1, 2, 3, \cdots \frac{Q-1}{2}$ positiv werden. Offenbar ist, da für jeden der $\frac{Q-1}{2}$ Werte des k entweder $\frac{hQ-kP}{PQ}$ oder $\frac{kP-hQ}{PQ}$ positiv werden mufs,

$$Ap_k\cdot\left(\frac{hQ-kP}{PQ}\right) + Ap_k\cdot\left(\frac{kP-hQ}{PQ}\right) = \frac{Q-1}{2};$$

man kann daher der Formel (125) auch die einfachere Gestalt

$$(126)\qquad \text{sgn. } R\left(\frac{hQ}{P}\right) = (-1)^{Ap_k\cdot\left(\frac{hQ+kP}{PQ}-\frac{1}{2}\right) - Ap_k\cdot\left(\frac{hQ-kP}{PQ}\right)}$$
$$= (-1)^{Ap_k\cdot\left(\frac{h}{P}+\frac{k}{Q}-\frac{1}{2}\right) - Ap_k\cdot\left(\frac{h}{P}-\frac{k}{Q}\right)},$$

oder auch, da das Vorzeichen eines Ausdrucks sich nicht ändert, wenn er durch einen positiven Wert multipliziert oder dividiert wird, die folgende:

$$(127)\qquad \text{sgn. } R\left(\frac{hQ}{P}\right) = (-1)^{Ap_k\cdot\left(hQ+kP-\frac{PQ}{2}\right) - Ap_k\cdot(hQ-kP)}$$

erteilen.

Diese, aus einer nicht arithmetischen Quelle erschlossene Formel hat nun a. a. O. Genocchi auch arithmetisch begründet. In der That wird $hQ - kP > 0$, solange $k < \frac{hQ}{P}$ d. i. $\overline{\gtrless}\left[\frac{hQ}{P}\right]$ ist, mithin besteht die Gleichung

$$(128)\qquad Ap_k\cdot(hQ-kP) = Ap_k\cdot\left(\frac{h}{P}-\frac{k}{Q}\right) = \left[\frac{hQ}{P}\right].$$

Desgleichen wird $hQ + kP - \frac{PQ}{2} > 0$, sobald $k > \frac{Q}{2} - \frac{hQ}{P}$ d. i. $> \frac{Q-1}{2} + \frac{1}{2} - \frac{hQ}{P}$ ist, also, falls $R\left(\frac{hQ}{P}\right) > 0$ ist, für $k > \frac{Q-1}{2} - \left[\frac{hQ}{P}\right]$, falls aber $R\left(\frac{hQ}{P}\right) < 0$ ist, für $k \overline{\gtrless} \frac{Q-1}{2} - \left[\frac{hQ}{P}\right]$; demnach ist die

Anzahl der zulässigen k je nach diesen beiden Fällen gleich $\left[\frac{hQ}{P}\right]$ resp. gleich $\left[\frac{hQ}{P}\right]+1$, und somit besteht die Gleichung

$$(129)\qquad Ap_k\cdot\left(hQ+kP-\frac{PQ}{2}\right)=Ap_k\cdot\left(\frac{h}{P}+\frac{k}{Q}-\frac{1}{2}\right)=\left[\frac{hQ}{P}+\frac{1}{2}\right].$$

Der Exponent von -1 in der Formel (126), d. i. der Überschufs der Anzahl positiver Werte von $\frac{h}{P}+\frac{k}{Q}-\frac{1}{2}$ für $k=1,2,3,\cdots\frac{Q-1}{2}$ über die Anzahl positiver Werte von $\frac{h}{P}-\frac{k}{Q}$ für die gleichen Werte des k beträgt demnach

$$\left[\frac{hQ}{P}+\frac{1}{2}\right]-\left[\frac{hQ}{P}\right]$$

d. i. Null oder Eins, jenachdem $R\left(\frac{hQ}{P}\right)>0$ oder <0 ist; da entsprechend sgn. $R\left(\frac{hQ}{P}\right)=+1$ oder -1 ist, so ist also die Formel (126) oder (127) bewiesen.

Ehe wir weitergehen, wollen wir beiläufig an die Formeln (128), (129) eine bemerkenswerte Folgerung knüpfen. Setzt man in der Formel (129) für h die Werte $1,2,3,\cdots\frac{P-1}{2}$ und summiert, so erhält man

$$Ap_{h,k}\cdot\left(\frac{h}{P}+\frac{k}{Q}-\frac{1}{2}\right)=\sum_{h=1}^{\frac{P-1}{2}}\left[\frac{hQ}{P}+\frac{1}{2}\right],$$

wo nun links diejenige Anzahl steht, wie oft der Ausdruck $\frac{h}{P}+\frac{k}{Q}-\frac{1}{2}$ bei allen Kombinationen der Werte

$$h=1,2,3,\cdots\frac{P-1}{2};\qquad k=1,2,3,\cdots\frac{Q-1}{2}$$

positiv wird. Aus der Symmetrie des Ausdrucks in Bezug auf die Elemente P, Q und entsprechend in Bezug auf h, k ergiebt sich aber ebenso

$$Ap_{h,k}\left(\frac{h}{P}+\frac{k}{Q}-\frac{1}{2}\right)=\sum_{k=1}^{\frac{Q-1}{2}}\left[\frac{kP}{Q}+\frac{1}{2}\right]$$

und folglich die interessante Beziehung:

$$(130)\qquad \sum_{h=1}^{\frac{P-1}{2}}\left[\frac{hQ}{P}+\frac{1}{2}\right]=\sum_{k=1}^{\frac{Q-1}{2}}\left[\frac{kP}{Q}+\frac{1}{2}\right].$$

Ähnlicherweise liefert die Formel (128) die Summationsgleichung

$$Ap_{h,k}\cdot\left(\frac{h}{P}-\frac{k}{Q}\right)=\sum_{h=1}^{\frac{P-1}{2}}\left[\frac{hQ}{P}\right],$$

der man die analoge andere:

$$Ap_{h,k}\cdot\left(\frac{k}{Q}-\frac{h}{P}\right)=\sum_{k=1}^{\frac{Q-1}{2}}\left[\frac{kP}{Q}\right]$$

an die Seite stellen kann. Addiert man beide und bedenkt, dafs für jede der $\frac{P-1}{2}\cdot\frac{Q-1}{2}$ Kombinationen der Werte von h und k einer der entgegengesetzten Ausdrücke $\frac{h}{P}-\frac{k}{Q}$, $\frac{k}{Q}-\frac{h}{P}$ notwendig positiv, der andere negativ werden und somit

$$Ap_{h,k}\cdot\left(\frac{h}{P}-\frac{k}{Q}\right)+Ap_{h,k}\cdot\left(\frac{k}{Q}-\frac{h}{P}\right)=\frac{P-1}{2}\cdot\frac{Q-1}{2}$$

sein mufs, so folgt eine zweite, der vorigen korrespondierende Formel:

$$(131)\qquad \sum_{h=1}^{\frac{P-1}{2}}\left[\frac{hQ}{P}\right]+\sum_{k=1}^{\frac{Q-1}{2}}\left[\frac{kP}{Q}\right]=\frac{P-1}{2}\cdot\frac{Q-1}{2}\ {}^{*)}.$$

Kehren wir nun zu unserm Gegenstande zurück, so ersehen wir aus (126), dafs die Formel (87) sich folgendermafsen schreiben läfst:

$$\left(\frac{Q}{P}\right)=(-1)^{Ap_{h,k}\cdot\left(\frac{h}{Q}+\frac{k}{P}-\frac{1}{2}\right)-Ap_{h,k}\cdot\left(\frac{h}{P}-\frac{k}{Q}\right)};$$

ebenso aber findet sich

$$\left(\frac{P}{Q}\right)=(-1)^{Ap_{h,k}\cdot\left(\frac{h}{Q}+\frac{k}{P}-\frac{1}{2}\right)-Ap_{h,k}\cdot\left(\frac{k}{Q}-\frac{h}{P}\right)},$$

und aus der Multiplikation dieser beiden Gleichungen, wenn man den Exponenten von -1 durch seinen Rest (mod. 2) ersetzt,

$$\left(\frac{P}{Q}\right)\cdot\left(\frac{Q}{P}\right)=(-1)^{Ap_{h,k}\cdot\left(\frac{h}{P}-\frac{k}{Q}\right)+Ap_{h,k}\cdot\left(\frac{k}{Q}-\frac{h}{P}\right)}$$

d. i. nach einer eben gemachten Bemerkung

$$\left(\frac{P}{Q}\right)\cdot\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}. —$$

---

*) S. zu diesen Formeln, auf welche wir später zurückkommen wollen, Hacks, *Acta Math.* 12, p. 109 ff., sowie Kronecker, *Berl. Sitzgsber.* 1885, p. 383.

Mit diesem Beweise von **Genocchi**, bezüglich dessen noch auf seine Bemerkungen in *Par. C. R.* 90, 1880, p. 300 und 101, 1885, p. 425 verwiesen sei, stimmt derjenige von **Schering** (*Gött. Nachr.* 1879) im Wesentlichen völlig überein, nur dafs sein Ausgangspunkt ein wenig allgemeiner ist. Schering hat in einer gröfseren Arbeit „*über die Bestimmung des quadratischen Restcharakters*“ (*Abh. der Göttinger Ges.* 24, 1879) für einen beliebigen reellen Wert x folgende Formeln aufgestellt:

$$(132)\quad \begin{cases} \mathfrak{B}(x) = x - Ap\cdot(x-k) + An\cdot(x-1+k) - Ao\cdot(x-k), \\ \mathfrak{AB}(x) = x - Ap\cdot(x+\frac{1}{2}-k) + An\cdot(x-\frac{1}{2}+k) + Ao\cdot(x-\frac{1}{2}+k), \\ \mathfrak{AB}(x) = x - Ap\cdot(x-k) + An\cdot(x-1+k) - Ao\cdot(x-k) - \alpha, \end{cases}$$
$$(\text{für } k = 1, 2, 3, 4, \ldots).$$

Hier bedeutet, wie vorher, $Ap\cdot(x-k)$ die Anzahl positiver Werte von $x-k$ für die angegebenen Werte von k, ebenso $An\cdot(x-1+k)$ die Anzahl negativer Werte von $x-1+k$, und $Ao\cdot(x-k)$ die Anzahl der Werte $x-k$, welche Null sind, u. s. w.; $\mathfrak{B}(x)$ ist der sogenannte „Bruchrest“ von x, d. h.

$$(133)\qquad \mathfrak{B}(x) = x - [x],$$

während $\mathfrak{AB}(x)$ dasselbe bedeutet, wie das Kroneckersche $R(x)$, nämlich

$$(134)\qquad \mathfrak{AB}(x) = x - \left[x + \frac{1}{2}\right];$$

endlich ist $\alpha = 0$ oder 1, jenachdem $\mathfrak{AB}(x) = R(x) \overline{>} 0$ oder < 0 ist. Beschränkt man in diesen Formeln, an welche wir bald wieder erinnern müssen, x auf positive, nicht ganzzahlige Werte, so besagen sie ganz einfach, wenn man auf (133), (134) achtet, dafs

$$Ap\cdot(x-k) = [x],\; Ap\cdot\left(x+\frac{1}{2}-k\right) = \left[x+\frac{1}{2}\right]$$

ist, was man auch unmittelbar als richtig anerkennt. Da nun aber

$$\left[x+\frac{1}{2}\right] - [x]$$

gleich Null oder Eins ist, jenachdem $R(x) > 0$ oder < 0 d. h. jenachdem sgn. $R(x) = +1$ oder -1 ist, ergiebt sich sogleich die Scheringsche Bestimmung:

$$(135)\qquad \text{sgn. } R.(x) = (-1)^{Ap\cdot(x+\frac{1}{2}-k) - Ap\cdot(x-k)},$$

welche an Stelle der ursprünglichen Gaufsschen in (108) oder (109) tritt. Für den Beweis des Reziprozitätsgesetzes genügt es, den Wert $x = \frac{hQ}{P}$ zu betrachten, wodurch man zu der Formel

$$(136) \qquad \text{sgn. } R\left(\frac{hQ}{P}\right) = (-1)^{Ap\cdot\left(\frac{hQ}{P}+\frac{1}{2}-k\right) - Ap\cdot\left(\frac{hQ}{P}-k\right)}$$

gelangt, in welcher man die unendliche Reihe der k auch auf die Werte $1, 2, 3, \cdots \left[\frac{hQ}{P}+\frac{1}{2}\right]$ beschränken darf; indem wir für h die Werte $1, 2, 3, \cdots \frac{P-1}{2}$ zu betrachten haben, erstrecken wir sie auf die längste der entsprechenden Reihen, welche $h = \frac{P-1}{2}$ zugehört und höchstens $1, 2, 3, \cdots \cdot \frac{Q-1}{2}$ ist. Da jedoch, wenn $k = \frac{Q+1}{2} - k'$ gesetzt wird, k' zugleich mit k, nur in umgekehrter Folge, diese Werte durchläuft, und wegen

$$\frac{hQ}{P} + \frac{1}{2} - k = Q\left(\frac{h}{P} + \frac{k'}{Q} - \frac{1}{2}\right)$$

jedem k, welches dem Ausdruck zur Linken ein bestimmtes Vorzeichen giebt, ein k' entspricht, für welches der Ausdruck $\frac{h}{P}+\frac{k'}{Q}-\frac{1}{2}$ dasselbe Vorzeichen erhält, und umgekehrt, so darf man die Gleichung (136) auch durch die andere:

$$\text{sgn. } R\left(\frac{hQ}{P}\right) = (-1)^{Ap\cdot\left(\frac{h}{P}+\frac{k}{Q}-\frac{1}{2}\right) - Ap\cdot\left(\frac{h}{P}-\frac{k}{Q}\right)}$$

ersetzen. Aus ihr, die mit der Formel (126) identisch ist, schliefst man dann, ganz wie Genocchi, das verallgemeinerte Reziprozitätsgesetz.

14. Bedenkt man, dafs, jenachdem x positiv oder negativ ist,

$$\frac{1}{2}(1 + \text{sgn. } x) = 1 \text{ oder } 0,$$

dagegen

$$\frac{1}{2}(1 - \text{sgn. } x) = 0 \text{ oder } 1$$

ist, so lassen sich die Formeln (128), (129), sowie der die Formel (126) aussprechende Satz der vorigen Nummer in der uns bereits vertrauteren Kroneckerschen Schreibweise folgendermafsen fassen:

$$(137) \qquad \begin{cases} \frac{1}{2}\sum_{k=1}^{\frac{Q-1}{2}}\left(1 + \text{sgn. } \left(\frac{h}{P}+\frac{k}{Q}-\frac{1}{2}\right)\right) = \left[\frac{hQ}{P}+\frac{1}{2}\right] \\ \frac{1}{2}\sum_{k=1}^{\frac{Q-1}{2}}\left(1 + \text{sgn. } \left(\frac{h}{P}-\frac{k}{Q}\right)\right) = \left[\frac{hQ}{P}\right] \end{cases}$$

und

$$(138)\quad \frac{1}{2}\sum_{k=1}^{\frac{Q-1}{2}}\left(1+\text{sgn.}\left(\frac{h}{P}+\frac{k}{Q}-\frac{1}{2}\right)\right)-\frac{1}{2}\sum_{k=1}^{\frac{Q-1}{2}}\left(1+\text{sgn.}\left(\frac{h}{P}-\frac{k}{Q}\right)\right)$$
$$=\frac{1}{2}\left(1-\text{sgn.}\,R\left(\frac{hQ}{P}\right)\right).$$

Aus der letzten dieser Formeln geht dann durch Summation über die Werte $h=1, 2, 3, \cdots \frac{P-1}{2}$ die weitere hervor:

$$\frac{1}{2}\sum_{h,k}\left(1+\text{sgn.}\left(\frac{h}{P}+\frac{k}{Q}-\frac{1}{2}\right)\right)-\frac{1}{2}\sum_{h,k}\left(1+\text{sgn.}\left(\frac{h}{P}-\frac{k}{Q}\right)\right)$$
$$=\frac{1}{2}\sum_{h=1}^{\frac{P-1}{2}}\left(1-\text{sgn.}\,R\left(\frac{hQ}{P}\right)\right),$$

in welcher die Doppelsummen sich über alle Kombinationen der Werte $h=1, 2, 3, \cdots \frac{P-1}{2}$; $k=1, 2, 3, \cdots \frac{Q-1}{2}$ erstrecken; gleicherweise aber ist

$$\frac{1}{2}\sum_{h,k}\left(1+\text{sgn.}\left(\frac{k}{Q}+\frac{h}{P}-\frac{1}{2}\right)\right)-\frac{1}{2}\sum_{h,k}\left(1+\text{sgn.}\left(\frac{k}{Q}-\frac{h}{P}\right)\right)$$
$$=\frac{1}{2}\sum_{k=1}^{\frac{Q-1}{2}}\left(1-\text{sgn.}\,R\left(\frac{kP}{Q}\right)\right),$$

und nun ergiebt sich aus der Addition der beiden letzten Gleichungen die (mod. 2) geltende Kongruenz:

$$\frac{1}{2}\sum_{h,k}\left(1+\text{sgn.}\left(\frac{h}{P}-\frac{k}{Q}\right)\right)+\frac{1}{2}\sum_{h,k}\left(1+\text{sgn.}\left(\frac{k}{Q}-\frac{h}{P}\right)\right)$$
$$\equiv\frac{1}{2}\sum_{h=1}^{\frac{P-1}{2}}\left(1-\text{sgn.}\,R\left(\frac{hQ}{P}\right)\right)+\frac{1}{2}\sum_{k=1}^{\frac{Q-1}{2}}\left(1-\text{sgn.}\,R\left(\frac{kP}{Q}\right)\right)$$

d. h., da für jede der $\frac{P-1}{2}\cdot\frac{Q-1}{2}$ Kombinationen h, k je eine der beiden Gröfsen

$$\frac{1}{2}\left(1+\text{sgn.}\left(\frac{h}{P}-\frac{k}{Q}\right)\right),\ \frac{1}{2}\left(1+\text{sgn.}\left(\frac{k}{Q}-\frac{h}{P}\right)\right)$$

gleich 1, die andere gleich 0 ist, die Kongruenz

$$\frac{1}{2}\sum_{h=1}^{\frac{P-1}{2}}\left(1-\text{sgn.}\,R\left(\frac{hQ}{P}\right)\right)+\frac{1}{2}\sum_{k=1}^{\frac{Q-1}{2}}\left(1-\text{sgn.}\,R\left(\frac{kP}{Q}\right)\right)$$
$$\equiv\frac{P-1}{2}\cdot\frac{Q-1}{2}\pmod{2},$$

welche nach Schlufs von Nr. 10 dem Reziprozitätsgesetze äquivalent ist (s. Kronecker, *Berl. Sitzungsber.* 1885, p. 383).

Neben dieser, nur in der Ausdrucksweise von Genocchi's und Schering's verschiedenen Kroneckerschen Herleitung des Reziprozitätsgesetzes hat Kronecker noch andere Varianten jener Beweise gegeben. Wie leicht einzusehen, ist die Scheringsche Bestimmung (135) des Zeichens sgn. $R(x)$ mit der folgenden identisch:

$$\text{(139)} \qquad \operatorname{sgn.} R(x) = \operatorname{sgn.} \prod (x-k)\left(x+\frac{1}{2}-k\right).$$

In der That wird für ein positives nicht ganzzahliges x der allgemeine Faktor des Produktes,

$$(x-k)\left(x+\frac{1}{2}-k\right),$$

positiv sein, sobald $k \overline{\gtrless} [x]$ und sobald $k > \left[x+\frac{1}{2}\right]$ ist; ist demnach $\left[x+\frac{1}{2}\right] = [x]$, was der Fall ist, wenn sgn. $R(x) = +1$ ist, so sind alle Faktoren des Produktes positiv und daher die rechte Seite von (139) gleich $+1$; wenn dagegen $\left[x+\frac{1}{2}\right] = [x]+1$ ist, was geschieht, wenn sgn. $R(x) = -1$ ist, so ist ein einziger Faktor des Produktes negativ, nämlich derjenige, welcher $k = \left[x+\frac{1}{2}\right]$ entspricht, und die rechte Seite von (139) ist gleich -1; die Formel (139) ist also begründet. — Im besonderen geht aus ihr für $x = \frac{hQ}{P}$ die andere hervor:

$$\operatorname{sgn.} R\left(\frac{hQ}{P}\right) = \operatorname{sgn.} \prod_k \left(\frac{hQ}{P}-k\right)\left(\frac{hQ}{P}+\frac{1}{2}-k\right).$$

Es genügt dabei wieder, bei der Multiplikation die Werte $k = 1, 2, 3, \cdots \left[\frac{hQ}{P}+\frac{1}{2}\right]$ zu umfassen, und wir erstrecken dieselbe daher, um dies für jeden der in betracht kommenden Werte des h zu erreichen, auf die Reihe $k = 1, 2, 3, \cdots \frac{Q-1}{2}$. Dann gewinnt man durch dieselbe Betrachtung wie bei Schering die folgende Gleichung

$$\text{(140)} \qquad \operatorname{sgn.} R\left(\frac{hQ}{P}\right) = \operatorname{sgn.} \prod_k \left(\frac{h}{P}-\frac{k}{Q}\right)\cdot\left(\frac{h}{P}+\frac{k}{Q}-\frac{1}{2}\right)$$

daher ferner

$$\text{(141)} \qquad \left(\frac{Q}{P}\right) = \operatorname{sgn.} \prod_{h,k} \left(\frac{h}{P}-\frac{k}{Q}\right)\left(\frac{h}{P}+\frac{k}{Q}-\frac{1}{2}\right),$$

desgleichen

$$\left(\frac{P}{Q}\right) = \operatorname{sgn.} \prod_{h,k} \left(\frac{k}{Q}-\frac{h}{P}\right)\left(\frac{h}{P}+\frac{k}{Q}-\frac{1}{2}\right)$$

also

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \operatorname{sgn.} \prod_{h,k} \left(\frac{h}{P}-\frac{k}{Q}\right)\left(\frac{k}{Q}-\frac{h}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

(s. Kronecker, *Berl. Sitzungsber.* 1884, p. 519, oder *J. f. Math.* 96, 1884, p. 348).

Kronecker hat a. a. O. auch gezeigt, dafs die Formel (141) durch eine wesentlich einfachere ersetzt werden kann. In dem Produkte

$$\prod_{h,k}\left(\frac{h}{P}+\frac{k}{Q}-\frac{1}{2}\right)$$

sind von den Faktoren, die einem bestimmten h entsprechen, alle diejenigen negativ, in denen $k \overline{\gtrless} \left[\frac{Q}{2}-\frac{hQ}{P}\right]$ ist; jener Zahl h gehören also $\left[\frac{Q}{2}-\frac{hQ}{P}\right]$ negative Faktoren zu, und demnach ist

$$\text{(142)} \qquad \text{sgn.} \prod_{h,k}\left(\frac{h}{P}+\frac{k}{Q}-\frac{1}{2}\right) = (-1)^{\sum\limits_{h=1}^{\frac{P-1}{2}}\left[\frac{Q}{2}-\frac{hQ}{P}\right]}.$$

Hier ist nun

$$\frac{Q}{2}-\frac{hQ}{P} = \frac{Q+1}{2}-\left(\frac{hQ}{P}+\frac{1}{2}\right)$$

also

$$\text{(143)} \qquad \left[\frac{Q}{2}-\frac{hQ}{P}\right] = \frac{Q-1}{2}-\left[\frac{hQ}{P}+\frac{1}{2}\right];$$

andererseits folgt aus $x-\left[x+\frac{1}{2}\right]=R\,(x)$ die Beziehung

$$h\,Q = P\cdot\left[\frac{hQ}{P}+\frac{1}{2}\right]+P\cdot R\left(\frac{hQ}{P}\right),$$

welche, mit der Kongruenz

$$h\,Q \equiv h'\cdot \text{sgn. } R\left(\frac{hQ}{P}\right) \pmod{P}$$

verglichen, weil $R\left(\frac{hQ}{P}\right)\cdot P$ absolut kleiner ist als $\frac{P}{2}$, in

$$\text{(144)} \qquad h\,Q = P\cdot\left[\frac{hQ}{P}+\frac{1}{2}\right]+h'\cdot \text{sgn. } R\left(\frac{hQ}{P}\right)$$

übergeht und die Kongruenz liefert:

$$\text{(145)} \qquad h \equiv \left[\frac{hQ}{P}+\frac{1}{2}\right]+h' \pmod{2}.$$

Da nun, wenn h die Werte $1, 2, 3, \cdots \frac{P-1}{2}$ durchläuft, auch h' diese Werte, wenn auch in einer anderen Reihenfolge, durchläuft, so findet sich aus (145) sogleich die beachtenswerte Kongruenz

$$\text{(146)} \qquad \sum_{h=1}^{\frac{P-1}{2}}\left[\frac{hQ}{P}+\frac{1}{2}\right] \equiv 0 \pmod{2}$$

und ihr zufolge aus (143) diese andere:

$$\sum_{h=1}^{\frac{P-1}{2}} \left[\frac{Q}{2} - \frac{hQ}{P}\right] \equiv \frac{P-1}{2} \cdot \frac{Q-1}{2} \pmod{2}.$$

Dadurch aber nimmt die Gleichung (142) die Gestalt an:

$$\operatorname{sgn.} \prod_{h,k} \left(\frac{h}{P} + \frac{k}{Q} - \frac{1}{2}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}},$$

weshalb es gestattet ist, die Gleichung (141) durch die nachstehende zu ersetzen:

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}} \cdot \operatorname{sgn.} \prod_{h,k} \left(\frac{h}{P} - \frac{k}{Q}\right),$$

oder noch einfacher zu schreiben, wie folgt:

$$(147) \qquad \left(\frac{Q}{P}\right) = \operatorname{sgn.} \prod_{h,k} \left(\frac{k}{Q} - \frac{h}{P}\right).$$

Zur Herleitung dieser Formeln bedarf es aber garnicht der Gleichung (139), welche der Scheringschen Bestimmung des Zeichens sgn. $R(x)$ entspricht, sondern man kann sie aus der ursprünglichen Gaufsschen Bestimmungsweise des letzteren d. i. aus der Formel (108) durch die einfache Bemerkung finden, dafs offenbar für jedes positive, nicht ganzzahlige x, für welches auch $2x$ nicht ganzzahlig ist,

$$(148) \qquad (-1)^{[2x]} = \operatorname{sgn.} \prod_{i=1,2,3,4,\cdots} (i - 2x)$$

gesetzt werden darf; dabei braucht man die Multiplikation sogar nur soweit zu erstrecken, dafs die Werte $1, 2, 3, \cdots [2x]$ umfafst werden. Demgemäfs ist nach (110)

$$(149) \qquad \operatorname{sgn.} R\left(\frac{hQ}{P}\right) = \operatorname{sgn.} \prod_{i=1}^{Q-1} \left(\frac{i}{2} - \frac{hQ}{P}\right);$$

werden aber die geraden Werte $i = 2k$ von den ungeraden, welche $i = Q - 2k$ genannt werden können, wenn man beiderseits k von 1 bis $\frac{Q-1}{2}$ laufen läfst, unterschieden, so findet sich sogleich

$$\operatorname{sgn.} R\left(\frac{hQ}{P}\right) = \operatorname{sgn.} \prod_{k=1}^{\frac{Q-1}{2}} \left(\frac{k}{Q} - \frac{h}{P}\right)\left(\frac{1}{2} - \frac{h}{P} - \frac{k}{Q}\right)$$

d. i. die Formel, aus welcher (141) und weiterhin (147) geschlossen worden ist. —

15. Schon lange vor Kronecker hat Schaar (*Bull. de l'Ac. R. de Belgique*, 14 I, 1847, p. 79) genau die gleiche Beziehung (149) benutzt, um in ganz ähnlicher Weise das Reziprozitätsgesetz zu be-

weisen. In der That bemerkt er, dafs das Vorzeichen in der fundamentalen Kongruenz (78):

$$hQ \equiv \pm h' \pmod{P},$$

worin h, h' Zahlen der Reihe $1, 2, 3, \cdots \frac{P-1}{2}$ sind, ganz wie die Formel (149) aussagt, stets dasselbe sei, wie dasjenige des Produktes

$$\prod_{i=1}^{Q-1}(iP-2hQ)$$

und dafs somit das Vorzeichen von $\left(\frac{Q}{P}\right)$ mit dem des Produktes

$$\prod_{i=1,\, h=1}^{Q-1,\, \frac{P-1}{2}}(iP-2hQ)$$

übereinstimme. Gleicherweise mufs dasjenige von $\left(\frac{P}{Q}\right)$ mit dem Vorzeichen des Produktes

$$\prod_{g=1,\, k=1}^{P-1,\, \frac{Q-1}{2}}(gQ-2kP)$$

identisch sein. Trennt man nun in dem letzteren die geraden Werte $g = 2h$ von den ungeraden, welche $g = P - 2h$ genannt werden können, so zerfällt das Produkt, da für die Zahlen $Q - 2k$ die ungeraden Zahlen $< Q$ gesetzt werden dürfen, in die beiden Faktoren

$$\prod_{h=1,\, k=1}^{\frac{P-1}{2},\, \frac{Q-1}{2}}(2hQ-2kP), \quad \prod_{h=1,\, k=1}^{\frac{P-1}{2},\, \frac{Q-1}{2}}((2k-1)P-2hQ),$$

deren erster gleich

$$\prod_{h=1,\, k=1}^{\frac{P-1}{2},\, \frac{Q-1}{2}}(2kP-2hQ)\cdot(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$

gesetzt werden darf, und ist demnach, da die Zahlen $2k - 1$ und $2k$ zusammen die ganze Reihe $1, 2, 3, \cdots Q - 1$ erschöpfen, nichts anderes, als

$$(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\cdot\prod_{i=1,\, h=1}^{Q-1,\, \frac{P-1}{2}}(iP-2hQ).$$

Daraus folgt offenbar, dafs das Vorzeichen von $\left(\frac{P}{Q}\right)$ mit demjenigen von

$$(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\cdot\left(\frac{Q}{P}\right)$$

übereinstimmt, dafs also

$$\left(\frac{P}{Q}\right) \cdot \left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}$$

ist. —

Mit diesen Betrachtungen von Schaar kommen in der Hauptsache diejenigen überein, welche L. Gegenbauer in einer Arbeit in den *Wiener Ber.* 103, 1894, p. 285, gegeben hat. Da nämlich dem Gesagten zufolge

$$(150) \qquad \left(\frac{Q}{P}\right) = \text{sgn.} \prod_{i=1,\, h=1}^{Q-1,\, \frac{P-1}{2}} \left(\frac{i}{Q} - \frac{2h}{P}\right)$$

ist, die rechte Seite aber durch

$$\text{sgn.} \prod_{i=1,\, h=1}^{\frac{Q-1}{2},\, \frac{P-1}{2}} \left(\frac{2i}{Q} - \frac{2h}{P}\right)\left(\frac{2i-1}{Q} - \frac{2h}{P}\right)$$

oder durch

$$\text{sgn.} \prod_{i=1,\, h=1}^{\frac{Q-1}{2},\, P-1} \left(\frac{2i}{Q} - \frac{h}{P}\right) \cdot \prod_{i=1,\, h=1}^{\frac{Q-1}{2},\, \frac{P-1}{2}} \left(\frac{2i}{Q} - \frac{2h-1}{P}\right)\left(\frac{2i-1}{Q} - \frac{2h}{P}\right)$$

ersetzt und des ungeraden P wegen der allgemeine Faktor des ersten Produktes mit entgegengesetztem Vorzeichen genommen werden darf, so geht aus (150) die Beziehung

$$(151) \qquad \left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \text{sgn.} \prod_{i=1,\, h=1}^{\frac{Q-1}{2},\, \frac{P-1}{2}} \left(\frac{2i}{Q} - \frac{2h-1}{P}\right)\left(\frac{2i-1}{Q} - \frac{2h}{P}\right)$$

hervor, welche das Reziprozitätsgesetz in sich enthält; denn durch die Substitution

$$2i = Q - (2i' - 1),\ 2h - 1 = P - 2h',$$

bei welcher i', h' dieselben Werte durchlaufen, wie i, h resp., verwandelt sich der erste Faktor des allgemeinen Gliedes unter dem $\prod$zeichen in

$$\frac{2h'}{P} - \frac{2i'-1}{Q},$$

daher sind die $\frac{P-1}{2} \cdot \frac{Q-1}{2}$ ersten Faktoren in gewisser Reihenfolge den zweiten Faktoren entgegengesetzt gleich, also

$$(152) \qquad \text{sgn.} \prod_{i=1,\, h=1}^{\frac{Q-1}{2},\, \frac{P-1}{2}} \left(\frac{2i}{Q} - \frac{2h-1}{P}\right)\left(\frac{2i-1}{Q} - \frac{2h}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}.$$

Da Q ungerade, die Anzahl der Faktoren, aus welchen das Produkt in (150) besteht, also gerade ist, darf man diese Formel auch schreiben wie folgt:

$$\left(\frac{Q}{P}\right) = \text{sgn.} \prod_{i=1,\, h=1}^{Q-1,\, \frac{P-1}{2}} \left(\frac{2h}{P} - \frac{i}{Q}\right).$$

Hieraus geht ein neuer Ausdruck für $\left(\frac{Q}{P}\right)$ als Potenz von -1 hervor, wenn man bedenkt, daſs $\frac{2h}{P} - \frac{i}{Q}$ nur für die Werte $h = 1, 2, 3, \cdots \left[\frac{Pi}{2Q}\right]$ negativ ist; man schlieſst so in der That

$$(153) \qquad \left(\frac{Q}{P}\right) = (-1)^{\sum\limits_{i=1}^{Q-1} \left[\frac{Pi}{2Q}\right]}.$$

Auch auf Grund dieser Formel kann in einfacher Weise das Reziprozitätsgesetz bewiesen werden, wie Lucas, der übrigens die vorige Formel unmittelbarer aus dem Gauſsschen Lemma entnimmt, gezeigt hat (*Bull. de l'Ac. de St. Pét., nouv. série* 1, 1890, p. 495; s. auch *Assoc. Franç., Limoges*, XIX_1, 1890, p. 147; ebend. auch Matrot).

Ferner ist auf Grund von (128) und (129) die Formel (126) mit der folgenden:

$$\text{sgn. } R\left(\frac{hQ}{P}\right) = (-1)^{\left[\frac{hQ}{P} + \frac{1}{2}\right] - \left[\frac{hQ}{P}\right]}$$

identisch, und aus dieser folgt mit Rücksicht auf (87)

$$(154) \qquad \left(\frac{Q}{P}\right) = (-1)^{\sum\limits_{h=1}^{\frac{P-1}{2}} \left[\frac{hQ}{P} + \frac{1}{2}\right] - \sum\limits_{h=1}^{\frac{P-1}{2}} \left[\frac{hQ}{P}\right]},$$

aus welcher Formel, eben wie noch aus einer ähnlichen anderen, Gegenbauer (*Wiener Ber.* 90, 1884, p. 1026; 92, 1885, p. 876) auf's Neue das Reziprozitätsgesetz erschlossen hat. Die Vergleichung dieser Formel mit dem früheren Ausdrucke (113) für $\left(\frac{Q}{P}\right)$ bestätigt übrigens die schon bemerkte Thatsache, daſs

$$(155) \qquad \sum_{h=1}^{\frac{P-1}{2}} \left[\frac{hQ}{P} + \frac{1}{2}\right] \equiv 0 \pmod{2}$$

ist. Hiermit verbinden wir eine Folgerung, welche aus (152) durch ähnliche Überlegung, wie sie zur Formel (153) geführt hat, gezogen werden kann. Da nämlich die Ausdrücke

$$\frac{2i}{Q} - \frac{2h-1}{P}, \quad \frac{2i-1}{Q} - \frac{2h}{P}$$

negativ sind, solange $i < \frac{(2h-1)Q}{2P}$ resp. $i < \frac{hQ}{P} + \frac{1}{2}$ ist, ergiebt sich aus jener Formel die Kongruenz

$$\sum_{h=1}^{\frac{P-1}{2}} \left[\frac{(2h-1)Q}{2P}\right] + \sum_{h=1}^{\frac{P-1}{2}} \left[\frac{hQ}{P} + \frac{1}{2}\right] \equiv \frac{P-1}{2} \cdot \frac{Q-1}{2} \pmod{2},$$

welche wegen (155) durch die einfachere:

$$\sum_{h=1}^{\frac{P-1}{2}} \left[\frac{(2h-1)Q}{P}\right] \equiv \frac{P-1}{2} \cdot \frac{Q-1}{2} \pmod{2} \tag{156}$$

ersetzt werden kann (s. Stern, *J. f. Math.* 106, 1892, p. 337; Kronecker, ebendas. p. 346).

Endlich hat Gegenbauer, statt einen Ausdruck für das Symbol $\left(\frac{Q}{P}\right)$ zu benutzen, das Reziprozitätsgesetz auch durch Verbindung zweier solcher Ausdrücke, nämlich der Formeln (153) und (154) erhalten (*Wien. Ber.* 100, 1891, p. 855); statt der letztern Formel benutzen wir einfacher die Formel (113) und setzen demgemäſs sowohl

$$\mu(Q, P) \equiv \sum_{h=1}^{\frac{P-1}{2}} \left[\frac{hQ}{P}\right] \tag{157}$$

als auch

$$\mu(Q, P) \equiv \sum_{i=1}^{Q-1} \left[\frac{iP}{2Q}\right] \tag{158}$$

(mod. 2).

Der erstere Ausdruck läſst sich schreiben, wie folgt:

$$\sum_{h=1}^{\frac{P-1}{2}} \left[\frac{2hQ}{2P}\right] = \sum_{h=1}^{P-1} \left[\frac{hQ}{2P}\right] - \sum_{h=1}^{\frac{P-1}{2}} \left[\frac{(2h-1)Q}{2P}\right].$$

Wird hier in der zweiten Summe rechts h durch $\frac{P+1}{2} - h'$ ersetzt, wo h' dieselben Werte durchläuft wie h, so geht sie vermöge der aus (95) flieſsenden Beziehung

$$\left[\frac{(2h-1)Q}{2P}\right] = \left[\frac{Q+1}{2} - \left(\frac{h'Q}{P} + \frac{1}{2}\right)\right] = \frac{Q-1}{2} - \left[\frac{h'Q}{P} + \frac{1}{2}\right]$$

in den Ausdruck

$$\frac{P-1}{2} \cdot \frac{Q-1}{2} - \sum_{h=1}^{\frac{P-1}{2}} \left[\frac{hQ}{P} + \frac{1}{2}\right]$$

und somit (157) in die folgende Gestalt:

$$\mu(Q, P) \equiv \sum_{h=1}^{P-1} \left[\frac{hQ}{2P}\right] - \frac{P-1}{2} \cdot \frac{Q-1}{2} + \sum_{h=1}^{\frac{P-1}{2}} \left[\frac{hQ}{P} + \frac{1}{2}\right] \pmod{2}$$

d. h. mit Rücksicht auf (155) und (158) in die Beziehung

$$\mu(Q, P) \equiv \mu(P, Q) - \frac{P-1}{2} \cdot \frac{Q-1}{2} \pmod{2}$$

über, welche dem Reziprozitätsgesetze gleichbedeutend ist.

Noch liefert die Formel (158) einen neuen Ausdruck für $\left(\frac{Q}{P}\right)$, wenn man die Summe zur Rechten in die zwei anderen:

$$\sum_{i=1}^{\frac{Q-1}{2}} \left[\frac{iP}{2Q}\right] + \sum_{i=\frac{Q+1}{2}}^{Q-1} \left[\frac{iP}{2Q}\right]$$

zerlegt. Da durch die Substitution von $Q-i$ an Stelle von i mit Beachtung der Beziehung

$$\left[\frac{(Q-i)P}{2Q}\right] = \left[\frac{P+1}{2} - \left(\frac{iP}{2Q} + \frac{1}{2}\right)\right] = \frac{P-1}{2} - \left[\frac{iP}{2Q} + \frac{1}{2}\right]$$

die erstere Summe übergeht in

$$\frac{P-1}{2} \cdot \frac{Q-1}{2} - \sum_{i=\frac{Q+1}{2}}^{Q-1} \left[\frac{iP}{2Q} + \frac{1}{2}\right],$$

die andere in

$$\frac{P-1}{2} \cdot \frac{Q-1}{2} - \sum_{i=1}^{\frac{Q-1}{2}} \left[\frac{iP}{2Q} + \frac{1}{2}\right],$$

so findet sich im Ganzen

$$\mu(Q, P) \equiv \sum_{i=1}^{Q-1} \left[\frac{iP}{2Q} + \frac{1}{2}\right] \pmod{2}$$

oder

$$\left(\frac{Q}{P}\right) = (-1)^{\sum_{i=1}^{\frac{Q-1}{2}} \left[\frac{iP}{2Q} + \frac{1}{2}\right]}. \tag{159}$$

16. Alle im Vorigen skizzierten Beweise sind, wie bemerkt, ebenso wie auch der von Lerch (*Teixeira J.* 8, 1887, p. 137) gegebene, nur als Umformungen oder Abarten des dritten Gaufsschen Beweises zu betrachten. Die allereinfachste Gestalt aber er-

hält dieser Beweis, wenn man mit **Kronecker** die Formel (147) unmittelbar aus der **Gaufsschen** Bestimmung des Zeichens sgn. $R\left(\frac{hQ}{P}\right)$ entnimmt. Aus dieser Bestimmung flofs nämlich bereits ganz einfach die Formel (113):

$$\left(\frac{Q}{P}\right) = (-1)^{\sum\limits_{h=1}^{\frac{P-1}{2}}\left[\frac{hQ}{P}\right]};$$

andererseits läfst die Formel (128) oder die leichteste unmittelbare Überlegung erkennen, dafs

$$(160) \qquad (-1)^{\left[\frac{hQ}{P}\right]} = \text{sgn.}\prod_k \left(\frac{k}{Q} - \frac{h}{P}\right)$$

ist, wenn die Multiplikation sich mindestens auf alle $k < \frac{hQ}{P}$, also etwa auf die Werte $k = 1, 2, 3, \cdots \frac{Q-1}{2}$ erstreckt; somit folgt ohne weiteres

$$\left(\frac{Q}{P}\right) = \text{sgn.}\prod_{h=1,\ k=1}^{\frac{P-1}{2},\ \frac{Q-1}{2}} \left(\frac{k}{Q} - \frac{h}{P}\right)$$

d. i. die Formel (147). Diese aber lehrt sofort das Reziprozitätsgesetz, wenn sie mit der entsprechenden Formel

$$\left(\frac{P}{Q}\right) = \text{sgn.}\prod_{h=1,\ k=1}^{\frac{P-1}{2},\ \frac{Q-1}{2}} \left(\frac{h}{P} - \frac{k}{Q}\right)$$

verglichen wird (s. hierzu auch Kronecker, *Berl. Sitzgsber.* 1884, p. 645; 1885, p. 117). —

Hieran fügen sich passend noch ein paar ergänzende Bemerkungen von Schering (*Berl. Sitzgsber.* 1885, p. 113). Aus der Gleichung

$$hQ = kP + h' \cdot \text{sgn.}\ R\left(\frac{hQ}{P}\right)$$

schliefst man, wenn, wie bisher immer, Q ungerade gedacht wird, wie in Nr. 14 die Kongruenz

$$h \equiv k + h' \pmod{2},$$

und da die Gesamtheit der h' mit der Gesamtheit der h übereinstimmt, die andere, welche mit (155) identisch ist,

$$\sum k \equiv 0 \pmod{2};$$

wird dagegen die Zahl Q als gerade vorausgesetzt, so erhält man aus jener Gleichung die Kongruenz

$$0 \equiv k + h' \pmod{2}$$

und folglich

$$\sum k \equiv \sum h' \text{ d. i. } 1 + 2 + 3 + \cdots + \frac{P-1}{2}$$

mithin

$$\sum k \equiv \frac{P^2-1}{8} \pmod{2}.$$

Ferner ist, da $k = \left[\frac{hQ}{P}\right]$ oder $= \left[\frac{hQ}{P}\right] + 1$ ist, jenachdem sgn. $R\left(\frac{hQ}{P}\right) = 1$ oder -1 ist,

$$(-1)^k \cdot \text{sgn.}\, R\left(\frac{hQ}{P}\right) = (-1)^{\left[\frac{hQ}{P}\right]}$$

oder nach (160)

$$(-1)^k \cdot \text{sgn.}\, R\left(\frac{hQ}{P}\right) = \text{sgn.} \prod_k \left(\frac{k}{Q} - \frac{h}{P}\right)$$

folglich

$$(-1)^{\Sigma k} \cdot \prod_h \text{sgn.}\, R\left(\frac{hQ}{P}\right) = \text{sgn.} \prod_{h,k} \left(\frac{k}{Q} - \frac{h}{P}\right).$$

Mit Rücksicht auf die vorausgeschickten Kongruenzen ist daher für ungerade Q:

$$\prod_{h=1}^{\frac{P-1}{2}} \text{sgn.}\, R\left(\frac{hQ}{P}\right) = \text{sgn.} \prod_{h=1,\ k=1}^{\frac{P-1}{2},\ \frac{Q-1}{2}} \left(\frac{k}{Q} - \frac{h}{P}\right),$$

was nichts anderes ist als die Formel (147), dagegen für gerade Q:

$$\prod_{h=1}^{\frac{P-1}{2}} \text{sgn.}\, R\left(\frac{hQ}{P}\right) = (-1)^{\frac{P^2-1}{8}} \cdot \text{sgn.} \prod_{h=1,\ k=1}^{\frac{P-1}{2},\ \frac{Q-1}{2}} \left(\frac{k}{Q} - \frac{h}{P}\right). —$$

Wir dürfen diese Betrachtungen nicht abschliefsen, ohne noch Kronecker's scharfsinnige Bemerkung mitzuteilen (s. Kronecker, *Berl. Sitzgsber.* 1885, p. 1045) über das Verhältnis, in welchem der fünfte und dritte Gaufssche Beweis und die hier skizzierten Abarten des letztern zu einander stehen. Indem die Gesamtheit der letzteren von der Formel (87) Gebrauch machen, fassen sie das Reziprozitätsgesetz unter der ersten der in Nr. 10 angegebenen drei Formen, und es sind namentlich die Kroneckerschen Darstellungen, in denen die Produktform für die Symbole $\left(\frac{P}{Q}\right)$, $\left(\frac{Q}{P}\right)$ deutlich zum Ausdrucke kommt. Dagegen sehen wir in den Beweisen von Genocchi und von Schering statt der Produkte Potenzen von -1, in deren Exponenten gewisse Funktionen ebenderselben Ausdrücke additiv auftreten,

aus denen als Faktoren jene Produkte zusammengesetzt sind, und wir sehen so, namentlich in der Darstellung am Anfange von Nr. 14, diese Beweise auf die dritte, in (90) ausgedrückte Form des Reziprozitätsgesetzes hingeleitet, unter welcher es auch im fünften Gaufsschen Beweise erwiesen wird. Hierdurch erscheinen jene beiden, wie auch der letztgenannte Gaufssche Beweis als eine Art „logarithmischer Umgestaltung“ des dritten **Gaufsschen** Beweises oder besser der **Kroneckerschen** Darstellungen desselben.

Und in der That besteht nach Kronecker's Bemerkung für jedes reelle x die Gleichung

$$\log x - \log |x| = z\pi i,$$

wo z eine gerade oder ungerade Zahl ist, jenachdem $x > 0$ oder < 0 ist, also die Kongruenz

$$\frac{1}{\pi i} \cdot \log \cdot \mathrm{sgn.}\, x \equiv \frac{1}{2}\,(1 - \mathrm{sgn.}\, x) \pmod{2}.$$

Infolge dieser Beziehung findet sich

$$\frac{1}{\pi i} \cdot \log \prod_{h=1}^{\frac{P-1}{2}} \mathrm{sgn.}\, R\left(\frac{hQ}{P}\right) \cdot \prod_{k=1}^{\frac{Q-1}{2}} \mathrm{sgn.}\, R\left(\frac{kP}{Q}\right)$$
$$\equiv \sum_{h=1}^{\frac{P-1}{2}} \frac{1}{2}\left(1 - \mathrm{sgn.}\, R\left(\frac{hQ}{P}\right)\right) + \sum_{k=1}^{\frac{Q-1}{2}} \frac{1}{2}\left(1 - \mathrm{sgn.}\, R\left(\frac{kP}{Q}\right)\right) \pmod{2},$$

mithin ist die Kongruenz (90) nur die logarithmische Fassung der Gleichung (88), und dadurch nicht nur jenes Verhältnis der Beweise zu einander, sondern auch der Umstand klargelegt, weshalb der fünfte Gaufssche Beweis eine einfachere Grundlage hat, als der dritte.

17. Hier wird am Besten noch ein Beweis von **Kronecker** (*Berl. Monatsber.* 1876, p. 331) angeschlossen, den man mit **Hermes** als einen Beweis des Reziprozitätsgesetzes „durch Umkehrung“ bezeichnen kann. Auch **Hermes** gab einen solchen auf gleichem Grundgedanken beruhenden Beweis (Hermes, *Beweis des quadratischen Reziprozitätsgesetzes durch Umkehrung*, *Archiv f. Math. u. Phys.*, 2. Reihe, 5, 1887, p. 190), der jedoch wesentlich umständlicher ist, als der von Kronecker, und daher hier nur angeführt werden soll, um im übrigen den Leser auf ihn zu verweisen. Was diesen beiden Beweisen aufser ihrer eigentümlichen Methode besonderes Interesse verleiht, ist der Umstand, der sie dem ersten Gaufsschen Beweise nahe an die Seite stellt, dafs sie nicht nur auf das Prinzip der allgemeinen Induktion

zurückgreifen, sondern auch gerade wieder desjenigen Hilfssatzes bedürfen, der jenem zum Erfolge verhilft, des Satzes nämlich, dafs unterhalb jeder Primzahl p von der Form $8z+1$ eine ungerade Primzahl vorhanden ist, von welcher p quadratischer Nichtrest ist.

Für zwei positive ungerade, relativ prime Zahlen P, Q definiere man das Symbol (Q, P) durch die Gleichung

$$(161)\qquad (Q, P) = \text{sgn.}\prod_{h,k}\left(\frac{k}{Q}-\frac{h}{P}\right),$$

wo die Multiplikation sich auf alle Werte

$$h = 1, 2, 3, \dots \frac{P-1}{2};\qquad k = 1, 2, 3, \dots \frac{Q-1}{2}$$

erstreckt. Aus dieser Definitionsgleichung folgt sogleich die Beziehung

$$(162)\qquad (P, Q)\cdot(Q, P) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$

zwischen zwei „reciproken" Symbolen (P, Q), (Q, P). Desgleichen ersieht man unmittelbar, dafs

$$(163)\qquad (Q, P) = (-1)^{\sum\limits_{h=1}^{\frac{P-1}{2}}\left[\frac{hQ}{P}\right]}$$

ist. Bedeutet nun Q' eine zweite positive, ungerade, zu P prime Zahl, und ist, wenn $\varepsilon = \pm 1$ ist, die Kongruenz

$$(164)\qquad Q' \equiv \varepsilon Q \pmod{P}$$

erfüllt, so besteht auch eine Gleichung von der Form

$$Q' = \varepsilon Q + 2Pz,$$

und da nach (94) leicht sich

$$[\varepsilon x] \equiv [x] + \frac{1-\varepsilon}{2} \pmod{2}$$

herausstellt, findet man

$$\left[\frac{hQ'}{P}\right] \equiv \left[\frac{hQ}{P}\right] + \frac{1-\varepsilon}{2} \pmod{2}.$$

Da nun analog mit (163) für positive ungerade, zu P prime Q'

$$(165)\qquad (Q', P) = (-1)^{\sum\limits_{h=1}^{\frac{P-1}{2}}\left[\frac{hQ'}{P}\right]}$$

ist, geht unter Voraussetzung von (164) die Formel hervor:

$$(166)\qquad (Q', P) = (Q, P)\cdot(-1)^{\frac{P-1}{2}\cdot\frac{\varepsilon-1}{2}}.$$

Ferner ist nach (144)

$$hQ = P \cdot \left[\frac{hQ}{P} + \frac{1}{2}\right] + h' \cdot \text{sgn.}\, R\left(\frac{hQ}{P}\right),$$

während $\left[\frac{hQ}{P}+\frac{1}{2}\right]-\left[\frac{hQ}{P}\right]$ gleich 0 oder 1 ist, jenachdem sgn. $R\left(\frac{hQ}{P}\right)=+1$ oder -1 ist. Aus diesen Verhältnissen folgt im ersteren Falle:

$$\left[\frac{hQQ'}{P}\right] = Q' \cdot \left[\frac{hQ}{P}\right] + \left[\frac{h'Q'}{P}\right],$$

im zweiten:

$$\left[\frac{hQQ'}{P}\right] = Q' \cdot \left[\frac{hQ}{P}\right] + Q' - 1 - \left[\frac{h'Q'}{P}\right],$$

in beiden Fällen also:

$$\left[\frac{hQQ'}{P}\right] \equiv \left[\frac{hQ}{P}\right] + \left[\frac{h'Q'}{P}\right] \pmod{2}.$$

Bedenkt man nun, dafs h' gleichzeitig mit h die Werte $1, 2, 3, \cdots \frac{P-1}{2}$ in gewisser Reihenfolge durchläuft, so folgt mit Rücksicht auf die Formeln (163), (165), sowie auf die ihnen analoge:

$$(QQ', P) = (-1)^{\sum\limits_{h=1}^{\frac{P-1}{2}} \left[\frac{hQQ'}{P}\right]}$$

die neue Beziehung:

(167) $$(QQ', P) = (Q, P) \cdot (Q', P).$$

Da neben der Reziprozitätsgleichung (162) die beiden analogen:

$$(P, Q') \cdot (Q', P) = (-1)^{\frac{P-1}{2} \cdot \frac{Q'-1}{2}},$$

$$(P, QQ') \cdot (QQ', P) = (-1)^{\frac{P-1}{2} \cdot \frac{QQ'-1}{2}}$$

erfüllt sind, so fliefst hieraus mit Beachtung der Kongruenz

$$\frac{QQ'-1}{2} \equiv \frac{Q-1}{2} + \frac{Q'-1}{2} \pmod{2}$$

die fernere Gleichung

(168) $$(P, QQ') = (P, Q) \cdot (P, Q').$$

Diese für das Symbol (Q, P) ermittelten Beziehungen, welche völlig denjenigen entsprechen, die für das Jacobische Symbol $\left(\frac{Q}{P}\right)$ bestehen, lassen nun auch ohne Mühe die Identität beider Symbole erkennen und liefern so dann in der Gleichung (162) einen neuen Beweis des Reziprozitätsgesetzes.

In der That lehrt zunächst die letzte Gleichung, dafs die gedachte Übereinstimmung allgemein statthaben wird, sobald man sie

für Primzahlwerte des zweiten Argumentes nachweisen kann. Dies also nur bleibt zu leisten.

Nun folgt aber aus (167), weil das Symbol (Q, P) eine Einheit bedeutet, durch Gleichsetzung von Q' mit Q und wenn man P als eine positive ungerade Primzahl p voraussetzt, durch welche Q nicht aufgeht, die Gleichung

$$(Q^2, p) = 1. \tag{169}$$

Ist also R ein quadratischer Rest von p, sodaſs eine Kongruenz $Q^2 \equiv R \pmod{p}$ stattfindet, so folgt in Anbetracht von (164), (166)

$$(R, p) = 1, \text{ d. h. } (R, p) = \left(\frac{R}{p}\right).$$

Demnach kann (M, p) nur dann gleich -1 sein, wenn M ein quadratischer Nichtrest von p ist; wenn aber für *einen* solchen Nichtrest $(M, p) = -1$ also $(M, p) = \left(\frac{M}{p}\right)$ ist, so besteht derselbe Wert d. h. die Gleichheit $(N, p) = \left(\frac{N}{p}\right)$ für *jeden* Nichtrest N; denn, wäre im Gegenteil für einen solchen $(N, p) = +1$, so würde nach (167) $(MN, p) = -1$ sein, während doch MN ein quadratischer Rest von p wäre. Hiernach genügt es offenbar zu zeigen, daſs es eine Zahl M giebt (die dann ein quadratischer Nichtrest von p sein muſs), für welche $(M, p) = -1$ ist.

Da wegen (169) stets $(1, p) = +1$ ist, schlieſst man für Primzahlen $p = 4z + 3$ aus (166), wenn man $Q = 1$, $Q' = 2p - 1$ wählt

$$(2p - 1, p) = -1,$$

also ist in diesem Falle $M = 2p - 1$ eine Zahl, wie sie nachgewiesen werden soll.

Für eine Primzahl $p = 8z + 5$ hat $\frac{p+1}{2}$ die Form $4z + 3$; setzt man mithin $M = \frac{p+1}{2}$, so ist $p \equiv -1 \pmod{M}$ und dieselbe Formel (166) giebt, wenn darin $P = M$, $Q = 1$, $Q' = p$ gewählt wird,

$$(p, M) = -1,$$

wegen der Reziprozitätsformel (162) also auch

$$(M, p) = -1,$$

mithin ist in diesem Falle $M = \frac{p+1}{2}$ eine Zahl, wie sie nachgewiesen werden soll.

Ist endlich p eine Primzahl von der Form $8z + 1$, so wollen wir annehmen, für jede kleinere Primzahl von dieser Form sei die

Existenz einer solchen Zahl M bereits erwiesen. Dem Vorigen zufolge giebt es dann also für jede Primzahl p', welche kleiner als p, eine Zahl von der gedachten Art, und folglich sind für jede solche Primzahl p' die Symbole $\left(\frac{Q}{p'}\right)$ und (Q, p') identisch. Nun sei aber p' eine solche unterhalb p liegende Primzahl, von welcher p quadratischer Nichtrest also

$$(p, p') = \left(\frac{p}{p'}\right) = -1$$

ist, wie es sie nach dem eben in Erinnerung gebrachten Gaufsschen Hilfssatze stets giebt; dann folgt unmittelbar aus der Reziprozitätsformel (162)

$$(p', p) = -1,$$

also wäre $M = p'$ eine Zahl, wie sie nachzuweisen war, und man hätte demnach die Existenz einer solchen Zahl auch noch für die Primzahl p von der Form $8z + 1$, und, da dieser Schlufs immer wiederholt werden kann, für jede solche Primzahl bewiesen.

Hierdurch ist dann aber dem Gesagten zufolge auch das Reziprozitätsgesetz implicite mitbewiesen. —

18. Auf derselben Grundlage, wie der dritte **Gaufs**sche Beweis, aber mit anderen Hilfsmitteln operieren die Beweise des Reziprozitätsgesetzes, welche **E. Busche** gegeben hat. Der erste von ihnen findet sich in des genannten Verfassers Inauguraldissertation *„über eine Beweismethode in der Zahlentheorie“*, Göttingen 1883, ist aber auch in einer Abhandlung desselben *„über die Funktion* $\sum_{x=1}^{\frac{q-1}{2}}\left[\frac{px}{q}\right]$*“*, *J. f. Math.* 106, 1890, p. 65 begründet, auf deren Betrachtung und kurze Darstellung wir hier uns beschränken müssen. Das besondere Hilfsmittel, dessen sich Busche darin bedient, ist ein bemerkenswerter allgemeiner Satz, den wir hier nur in der Form und dem Umfange aussprechen wollen, in denen wir seiner bedürfen. So lautet er folgendermafsen:

Eine Relation $R(x, y)$ zwischen zwei Gröfsen x, y besteht für jedes Paar teilerfremder ungerader Zahlen $x = M$, $y = N$, wenn

1) aus ihrem Bestehen für ein solches Paar M, N auch ihr Bestehen für die Paare $M + 2\lambda N$, N und $M, N + 2\lambda M$ folgt, wobei λ ganzzahlig gedacht ist, und wenn

2) sie für die Werte $x = y = \varepsilon$ besteht, wo $\varepsilon = \pm 1$.

Zum Beweise dieses allgemeinen Satzes bilde man, wenn M, N zwei teilerfremde ungerade Zahlen bedeuten, einen Euclidischen Algorithmus mit geraden Quotienten:

$$(170)\qquad \begin{aligned} M &= 2\lambda N + M' \\ N &= 2\lambda' M' + M'' \\ M' &= 2\lambda'' M'' + M''' \\ &\cdots\cdots\cdots\cdots \\ M^{(i-2)} &= 2\lambda^{(i-1)} M^{(i-1)} + M^{(i)} \\ M^{(i-1)} &= 2\lambda^{(i)} M^{(i)} + M^{(i)}, \end{aligned}$$

sodafs die Zahlen $M, N, M', M'', \cdots$ abnehmende, positive oder negative, ungerade Zahlen sind, bis zu $M^{(i)} = \varepsilon$. Gilt nun, wie unter 2) angenommen, die Relation $R(x, y)$ für $x = y = M^{(i)}$ d. i. für das Paar teilerfremder ungerader Zahlen $M^{(i)}, M^{(i)}$, so gilt sie nach der Annahme 1) auch für die Paare

$$M^{(i-1)} = M^{(i)} + 2\lambda^{(i)} M^{(i)},\ M^{(i)}$$

und

$$M^{(i)},\ M^{(i)} + 2\lambda^{(i)} M^{(i)} = M^{(i-1)},$$

folglich nach derselben Annahme auch für die Paare

$$M^{(i-2)} = M^{(i)} + 2\lambda^{(i-1)} M^{(i-1)},\ M^{(i-1)}$$

$$M^{(i-1)},\ M^{(i)} + 2\lambda^{(i-1)} M^{(i-1)} = M^{(i-2)},$$

u. s. w., endlich auch für die Paare M, N und N, M, w. z. b. w.

Sind demnach $F(x, y)$, $F_1(x, y)$ zwei beliebige Funktionen von x, y, so besteht die Gleichheit

$$(171)\qquad F(M, N) = F_1(M, N)$$

für jedes Paar teilerfremder ungerader Zahlen M, N, wenn

1) für solche Paare die sogenannten Veränderungen beider Funktionen gleich sind d. h. wenn die Gleichungen bestehen

$$F(M + 2\lambda N, N) - F(M, N) = F_1(M + 2\lambda N, N) - F_1(M, N)$$

$$F(M, N + 2\lambda M) - F(M, N) = F_1(M, N + 2\lambda M) - F_1(M, N),$$

wobei λ ganzzahlig gedacht ist, und wenn

$$2)\qquad F(\varepsilon, \varepsilon) = F_1(\varepsilon, \varepsilon)$$

ist. In der That folgt wegen der ersten Annahme aus dem Bestehen der Gleichung (171) für ein solches Paar Zahlen M, N auch das Bestehen der Gleichungen

$$F(M + 2\lambda N, N) = F_1(M + 2\lambda N, N)$$

$$F(M, N + 2\lambda M) = F_1(M, N + 2\lambda M)$$

und somit nach dem Hilfssatze die Gleichung (171) für jedes Paar Zahlen der gedachten Art.

Dies vorausgeschickt, betrachten wir mit Busche den Summenausdruck

$$\psi(M,N) = \sum_{k=1}^{\frac{N-1}{2}} \left[\frac{Mk}{N}\right], \tag{172}$$

worin zunächst die teilerfremden ungeraden Zahlen M, N positiv gedacht sind. Um sodann die Funktion auch für negative Argumentwerte zu definieren, setzen wir fest, daſs

$$\psi(-M,N) = -\frac{N-1}{2} - \psi(M,N) \tag{172a}$$

$$\psi(\pm M, -N) = -\psi(\pm M, N) \tag{172b}$$

sein soll. Dann ergiebt sich für positive M, N und positive ganzzahlige λ ohne weiteres

$$\psi(M + 2\lambda N, N) = \sum_{k=1}^{\frac{N-1}{2}} \left[\frac{Mk}{N}\right] + 2\lambda\left(1 + 2 + \cdots + \frac{N-1}{2}\right)$$

mithin die erste Veränderung der Funktion:

$$\psi(M + 2\lambda N, N) - \psi(M,N) = \lambda \cdot \frac{N^2-1}{4}. \tag{173}$$

Ferner ist der Definition zufolge

$$\psi(M, N + 2\lambda M) = \sum_{k=1}^{\frac{N+2\lambda M-1}{2}} \left[\frac{Mk}{N+2\lambda M}\right]. \tag{174}$$

Nun zeigten wir bereits beim dritten Gauſsschen Beweise, daſs in der Summe (172) die Anzahl derjenigen Glieder, welche einer ganzen Zahl n der Reihe $0, 1, 2, \cdots \frac{M-3}{2}$ gleich sind, gleich

$$\left[\frac{(n+1)N}{M}\right] - \left[\frac{nN}{M}\right]$$

ist; aus derselben Erwägung wird die Anzahl solcher Glieder in der Summe (174) gleich

$$\left[\frac{(n+1)(N+2\lambda M)}{M}\right] - \left[\frac{n(N+2\lambda M)}{M}\right]$$

$$= \left[\frac{(n+1)N}{M}\right] - \left[\frac{nN}{M}\right] + 2\lambda(n+1) - 2\lambda n$$

sein und demnach jene Anzahl um 2λ übertreffen. Desgleichen wird die Anzahl der Glieder der ersteren Summe, welche den gröſsten Wert $\frac{M-1}{2}$ haben, gleich

$$\frac{N-1}{2} - \left[\frac{M-1}{2} \cdot \frac{N}{M}\right]$$

sein, und wird für die letztere Summe

$$\frac{N+2\lambda M-1}{2}-\left[\frac{M-1}{2}\cdot\frac{N+2\lambda M}{M}\right]$$
$$=\frac{N-1}{2}-\left[\frac{M-1}{2}\cdot\frac{N}{M}\right]+\lambda M-\lambda(M-1)$$

also um λ grösser sein, als jene Anzahl. Aus all' diesem geht hervor, dafs die letztere Summe die erstere um

$$2\lambda\left(1+2+\cdots+\frac{M-3}{2}\right)+\lambda\cdot\frac{M-1}{2}=\lambda\cdot\left(\frac{M-1}{2}\right)^2$$

übertrifft, und man findet somit als zweite Veränderung der Funktion $\psi(M,N)$:

$$\psi(M,N+2\lambda M)-\psi(M,N)=\lambda\cdot\left(\frac{M-1}{2}\right)^2. \tag{175}$$

Auf ähnliche Weise ergeben sich die beiden Formeln

$$\begin{aligned}\psi(-M+2\lambda N,N)-\psi(-M,N)&=\lambda\cdot\frac{N^2-1}{4}\\ \psi(M,-N+2\lambda M)-\psi(M,-N)&=\lambda\cdot\left(\frac{M-1}{2}\right)^2.\end{aligned} \tag{176}$$

Aus den so gewonnenen vier Grundformeln (173), (175), (176), in denen zunächst M, N und λ positiv gedacht sind, lassen sich nun die Veränderungen bei beliebigen Vorzeichen dieser Gröfsen gemäfs den Definitionsgleichungen (172), (172a, b) ermitteln. Indem wir der Kürze wegen in dieser Hinsicht den Leser auf die Abhandlung von Busche verweisen, teilen wir nur das allgemeine Endergebnis mit, zu welchem er gelangt. Setzt man

$$\begin{aligned}F(M,N)&=\psi(M,N)+\psi(N,M)=F(N,M)\\ f(M,N)&=\psi(M,N)-\psi(N,M)=-f(N,M),\end{aligned} \tag{177}$$

so ist für beliebige Vorzeichen der Zahlen M, N, λ

$$\begin{aligned}F(M+2\lambda N,N)-F(M,N)&=\lambda\cdot\frac{N(N-1)}{2}-\eta\\ f(M+2\lambda N,N)-f(M,N)&=\lambda\cdot\frac{N-1}{2}+\eta,\end{aligned} \tag{178}$$

worin η eine Gröfse ist, deren Wert durch die Formel

$$\eta=\frac{\operatorname{sgn.}N-1}{2}\left(\frac{\operatorname{sgn.}(M+2\lambda N)-1}{2}-\frac{\operatorname{sgn.}M-1}{2}\right) \tag{179}$$

bestimmt wird; die zweiten Veränderungen der Funktionen $F(M,N)$, $f(M,N)$ ergeben sich aus (178) mittels der Definitionsgleichungen (177).

Man beachte nun, dafs die Funktion

$$\frac{M-1}{2}\cdot\frac{N-1}{2}-\frac{\operatorname{sgn.}M-1}{2}\cdot\frac{\operatorname{sgn.}N-1}{2}, \tag{180}$$

wie sogleich zu übersehen, genau dieselben Veränderungen hat, wie die Funktion $F(M, N)$; für $M = N = \varepsilon$ ist sie Null; diesen Wert hat aber auch

$$F(\varepsilon, \varepsilon) = 2\,\psi(\varepsilon, \varepsilon),$$

wie für $\varepsilon = +1$ unmittelbar aus der Formel (172), für $\varepsilon = -1$ mit Hilfe der Definitionsgleichungen (172a, b) ohne Schwierigkeit erkannt wird. Dem vorausgeschickten Hilfssatze zufolge ist demnach für jedes Paar teilerfremder ungerader Zahlen M, N

$$(181) \qquad F(M, N) = \frac{M-1}{2} \cdot \frac{N-1}{2} - \frac{\text{sgn.}\, M - 1}{2} \cdot \frac{\text{sgn.}\, N - 1}{2}.$$

Sind im Besonderen $M = P$, $N = Q$ positive ungerade, relativ prime Zahlen, so bestehen nach (114) die Kongruenzen

$$\mu(Q, P) \equiv \psi(Q, P), \; \mu(P, Q) \equiv \psi(P, Q) \pmod{2}$$

und folglich

$$\mu(Q, P) + \mu(P, Q) \equiv F(P, Q) \pmod{2},$$

während aus (181)

$$F(P, Q) = \frac{P-1}{2} \cdot \frac{Q-1}{2}$$

hervorgeht. Demnach findet sich in der Formel

$$\mu(Q, P) + \mu(P, Q) \equiv \frac{P-1}{2} \cdot \frac{Q-1}{2} \pmod{2}$$

das Reziprozitätsgesetz aufs neue bewiesen.

Auch die Funktion $f(M, N)$ läfst sich auf Grund der aufgestellten Formeln berechnen. Aus dem Euclidischen Algorithmus (170) findet sich nämlich bei Beachtung der zweiten der Gleichungen (178) folgende Reihe von Gleichungen:

$$f(M, N) = f(M', N) + \lambda \cdot \frac{N-1}{2} + \eta'$$

$$f(M', N) = -f(M'', M') - \lambda' \cdot \frac{M'-1}{2} - \eta''$$

$$-f(M'', M') = f(M''', M'') + \lambda'' \cdot \frac{M''-1}{2} + \eta'''$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots,$$

in welchen $\eta', \eta'', \eta''', \cdots$ entsprechende Gröfsen sind, die nach dem Vorbilde der Gröfse η nach der Formel (179) gebildet sind, und aus ihnen geht schliefslich

$$f(M, N) = \lambda \cdot \frac{N-1}{2} - \lambda' \cdot \frac{M'-1}{2} + \lambda'' \cdot \frac{M''-1}{2} \cdots + \eta' - \eta'' + \eta''' - \cdots$$

hervor. Nun ist aber

$$\frac{1}{2}\left(\lambda N - \lambda' M' + \lambda'' M'' - \cdots\right) = \frac{1}{4}\left(2\lambda N - 2\lambda' M' + 2\lambda'' M'' - \cdots\right)$$
$$= \frac{1}{4}\left((M - M') - (N - M'') + (M' - M''') - (M'' - M^{(4)}) + \cdots\right)$$
$$= \frac{M - N}{4}$$

und somit darf man die vorige Formel einfacher schreiben, wie folgt:

$$(182)\quad f(M, N) = \frac{M - N}{4} - \frac{1}{2}(\lambda - \lambda' + \lambda'' - \cdots) + \eta' - \eta'' + \eta''' - \cdots.$$

Hat man aber durch die Formeln (181), (182) die Funktionen $F(M, N)$, $f(M, N)$ berechnet, so ergiebt sich nach (177) auch der Wert von $\psi(M, N)$ durch die Formel

$$(183)\qquad \psi(M, N) = \frac{1}{2}\left(F(M, N) + f(M, N)\right),$$

auf welche wir später noch zurückkommen werden.

19. Der andere Beweis **Busche**'s ist in seiner Arbeit „über gröfste Ganze", (*J. f. Math.* 103, 1888, p. 118) enthalten und bedient sich des Gaufsschen Lemma in einer neuen, modifizierten Gestalt. Wir haben letzteres in Nr. 12 in der Formel (113):

$$(184)\qquad \left(\frac{Q}{P}\right) = (-1)^{\sum\limits_{h=1}^{\frac{P-1}{2}}\left[\frac{hQ}{P}\right]}$$

ausgesprochen; im Exponenten dürfen wir aber diejenigen Glieder $\left[\frac{hQ}{P}\right]$, welche gerade sind, unterdrücken, und diejenigen, welche ungerade sind, durch Eins ersetzen, sodafs der Exponent dann die Anzahl der letzteren Glieder, d. i. die Anzahl der Vielfachen

$$(185)\qquad 1\cdot Q,\ 2\cdot Q,\ 3\cdot Q, \cdots \frac{P-1}{2}\cdot Q$$

angiebt, die zwischen einem ungeraden und dem darauf folgenden geraden Vielfachen von P enthalten sind. Man erhält also folgende Formulierung des verallgemeinerten Gaufsschen Lemma: Das Symbol $\left(\frac{Q}{P}\right)$ ist $+1$ oder -1, jenachdem die Anzahl der Vielfachen (185), welche je zwischen einem ungeraden und dem darauf folgenden geraden Vielfachen von P enthalten sind, gerade oder ungerade ist*).

---

*) Bei Busche sind die Vielfachen der Zahlen P, Q durch die ihrer Hälften $\frac{P}{2}$, $\frac{Q}{2}$ ersetzt, was indessen weder an dem Satze noch an dem darauf gegründeten Beweise etwas ändert; mit Hinsicht auf den folgenden Beweis von Lange sind wir darin von Jenem abgewichen.

Indem Busche diesen Satz direkt begründet und umgekehrt aus ihm die Formel (113) herleitet, gelangt er zuerst durch Anwendung einer allgemeinen in seiner Arbeit entwickelten Transformationsformel auf die in jener Formel enthaltene Summe oder auf das in der gleichbedeutenden Formel

$$\left(\frac{Q}{P}\right) = \prod_{h=1}^{\frac{P-1}{2}} (-1)^{\left[\frac{hQ}{P}\right]}$$

enthaltene Produkt zum Reziprozitätsgesetze, beweist dies sodann aber auch ohne jenes Hilfsmittel durch folgende einfache Erwägungen:

Wie bei den Beweisen von Fields und von Voigt stellen wir der Reihe von Vielfachen (185) von Q die Reihe

$$1 \cdot P,\ 2 \cdot P,\ 3 \cdot P, \cdots \frac{Q-1}{2} \cdot P \tag{186}$$

der Vielfachen von P gegenüber. Ist nun zunächst wenigstens eine der Zahlen P, Q von der Form $4z+1$, so sei dies Q. Die Vielfachen (186) zerfallen dann in $\frac{Q-1}{4}$ Paare $(2i-1)P$, $2iP$ aus einem ungeraden und dem darauf folgenden geraden Vielfachen von P. Liegt zwischen den Gliedern eines solchen Paares kein Vielfaches von Q, so sind umgekehrt jene Glieder zwischen zwei aufeinanderfolgenden Vielfachen von Q enthalten und liegen also entweder beide oder keins von ihnen zwischen einem ungeraden und dem darauf folgenden geraden Vielfachen von Q. Liegen dagegen zwischen $(2i-1)P$ und $2iP$ die Vielfachen

$$(k+1)Q, (k+2)Q, \cdots (k+k')Q$$

und ist die Anzahl dieser Vielfachen gerade, sodafs k und $k+k'$ gleichartig sind, so liegen, jenachdem k ungerade oder gerade ist, wieder beide Glieder des gedachten Paares oder keins von ihnen zwischen einem ungeraden und dem darauf folgenden geraden Vielfachen von Q. Wenn dagegen k' ungerade und folglich k, $k+k'$ ungleichartig sind, so liegt ein Glied jenes Paares zwischen einem ungeraden und dem darauf folgenden geraden Vielfachen von Q. Aus diesem gegenseitigen Verhalten der Reihen (185), (186) ist offenbar zu entnehmen, dafs in dem gegenwärtig betrachteten Falle die Anzahl der Vielfachen (186), welche zwischen einem ungeraden und dem darauf folgenden geraden Vielfachen von Q enthalten sind, immer zugleich mit der Anzahl der Vielfachen (185), die zwischen einem ungeraden und dem darauf folgenden geraden Vielfachen von P liegen, gerade oder zugleich mit ihr ungerade sein mufs. Des-

wegen ist aber dem modifizierten Gaufsschen Lemma zufolge in diesem Falle

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right).$$

Sind dagegen P, Q beide von der Form $4z + 3$, wo wir dann $P < Q$ annehmen wollen, so zerfallen die Vielfachen (186) in $\frac{Q-3}{4}$ Paare $(2i-1)P$, $2iP$ aus einem ungeraden und dem darauf folgenden geraden Vielfachen von P, zu denen noch ein letztes, isoliert stehendes Vielfaches $\frac{Q-1}{2} \cdot P$ hinzutritt. Bezüglich der gedachten Paare bleiben die vorigen Betrachtungen unverändert dieselben; das letztgenannte Vielfache von P aber liegt zwischen dem ungeraden Vielfachen $\frac{P-1}{2} \cdot Q$ und $\frac{PQ}{2}$, während zwischen dem ungeraden Vielfachen $\frac{Q-1}{2} \cdot P$ und $\frac{PQ}{2}$ kein Vielfaches von Q mehr liegen kann. Demnach mufs jetzt umgekehrt die Anzahl der Vielfachen (186), die zwischen einem ungeraden und dem darauf folgenden geraden Vielfachen von Q enthalten sind, gerade oder ungerade sein, jenachdem die Anzahl der Vielfachen (185), welche zwischen einem ungeraden und dem darauf folgenden geraden Vielfachen von P liegen, ungerade resp. gerade ist. Dem modifizierten Gaufsschen Lemma gemäfs ist also im jetzigen Falle

$$\left(\frac{Q}{P}\right) = -\left(\frac{P}{Q}\right).$$

Beide Fälle vereinigen sich in der Formel des Reziprozitätsgesetzes:

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}.$$

Wie Busche in einer weiteren Notiz (*Mitt. der math. Ges. in Hamburg*, III, Heft 6, 1896, p. 233), auf welche wir den Leser verweisen, gezeigt hat, kann sowohl das neue Gaufssche Lemma, als auch der darauf gegründete Beweis in sehr einfacher und gefälliger Weise geometrisch veranschaulicht werden.

20. In nächster Beziehung zu dem eben dargestellten Beweise von Busche steht derjenige Beweis, welchen Lange gegeben hat (Lange, *Ein elementarer Beweis des Reziprozitätsgesetzes*, *Ber. der K. Sächs. Ges.* 48, 1896, p. 629; 49, 1897, p. 607). Es sind eigentlich ihrer drei Beweise, doch ist der erste derselben im Grunde nur eine geometrisch anschauliche Darstellung des zweiten, der seinerseits im dritten eine sehr glückliche einfachere Fassung erhalten hat. Die beiden letzteren wollen wir hier entwickeln.

Auch sie beruhen auf einer besonderen Deutung des Gaufsschen Lemma, die sich leicht als identisch mit derjenigen von Busche erkennen läfst.

Die kleinsten positiven Reste (mod. P) der Reihe

(187) $$1 \cdot z,\ 2 \cdot z,\ 3 \cdot z, \cdots \frac{P-1}{2} \cdot z,$$

in welcher z eine beliebige positive, zu P prime Zahl bezeichne, sind teils kleiner als $\frac{P}{2}$, teils gröfser als $\frac{P}{2}$; u', g' seien die ungeraden und die geraden Reste der ersten, u'', g'' bezw. die der zweiten Kategorie, und $A_{u'}$, $A_{g'}, \cdots$ bezeichne die bezügliche Anzahl der Reste dieser einzelnen Kategorien. Der Definition der charakteristischen Zahl $\mu(Q, P)$ gemäfs ist dann

$$A_{u''} + A_{g''} = \mu(z, P);$$

da ferner, wie leicht zu übersehen ist, die u', g', $P-u''$, $P-g''$ zusammen die ganze Reihe der Zahlen $1, 2, 3, \cdots \frac{P-1}{2}$ ausmachen, so sind die u', $P-g''$ zusammen die ungeraden Zahlen $\overline{\gtrless} \frac{P-1}{2}$, mithin ist, jenachdem $\frac{P-1}{2}$ gerade oder ungerade ist,

$$A_{u'} + A_{g''} = \frac{P-1}{4} \text{ oder } \frac{P+1}{4}.$$

Bezeichnet man daher $A_{u'} + A_{u''}$ d. h. die Anzahl aller ungeraden Reste der Zahlen (187) (mod. P) mit u, so findet sich

$$u + 2\,A_{g''} = \frac{P \mp 1}{4} + \mu(z, P)$$

d. h.

$$\mu(z, P) \equiv u + \frac{P-1}{4} \cdot \frac{P+1}{2} \equiv u + \frac{P^2-1}{8} \pmod{2}$$

und folglich

(188) $$\left(\frac{z}{P}\right) = (-1)^{\frac{P^2-1}{8} + u}.$$

Setzen wir nun $z = 2\,Q$, wo Q eine positive ungerade zu P prime Zahl bedeute, so folgt zunächst

(189) $$\left(\frac{Q}{P}\right) = (-1)^u,$$

wenn u die Anzahl der ungeraden kleinsten positiven Reste in der Reihe

(190) $$2\,Q,\ 4\,Q,\ 6\,Q, \cdots (P-1)\,Q \pmod{P}$$

bedeutet. Unterscheidet man in dieser Reihe die Vielfachen von Q, welche $< \frac{PQ}{2}$ sind, von denjenigen, die $> \frac{PQ}{2}$ sind, so sind die ersteren die geraden Vielfachen der Reihe

(191) $$1 \cdot Q,\ 2 \cdot Q,\ 3 \cdot Q, \cdots \frac{P-1}{2}\,Q,$$

während die anderen, wenn sie in der Gestalt

$$(P-(2i-1))\,Q = Py + R$$

geschrieben werden, aus welcher

$$(2i-1)\,Q = P\,(Q-y-1) + (P-R)$$

folgt, erkennen lassen, dafs jedem von ihnen, dem ein ungerader kleinster positiver Rest R (mod. P) zugehört, ein ungerades Vielfaches der Reihe (191) entspricht, dem ein gerader Rest zugehört, und umgekehrt. Nennt man also v die Anzahl ungerader Reste auf den geraden Stellen, und w die Anzahl gerader Reste auf den ungeraden Stellen der Reihe (191), so ist $v+w$ gleich der Anzahl ungerader Reste in der Reihe (190) d. h. gleich u, und somit wegen (189) auch

$$(192)\qquad \left(\frac{Q}{P}\right) = (-1)^{v+w}.$$

Nun setze man

$$(193)\qquad \begin{gathered} h\,Q = \alpha_h \cdot P + \varrho_h \\ \left(h = 1, 2, 3, \ldots \frac{P-1}{2}\right), \end{gathered}$$

wo ϱ_h den positiven kleinsten Rest (mod. P) bedeutet; offenbar giebt $u = v + w$ die Anzahl der Fälle oder der Werte h an, für welche h und ϱ_h ungleichartig und folglich α_h ein ungerader Quotient ist, mit anderen Worten, die Anzahl der Fälle, wo das Vielfache $h\,Q$ zwischen einem ungeraden und dem darauf folgenden geraden Vielfachen von P enthalten ist, und demnach besagen die Formeln (189), (192) nichts anderes, als die dem Gaufsschen Lemma von Busche gegebene Deutung. So gestaltet sich denn auch der Langesche Beweis dem seinigen ganz analog.

Nimmt man dabei $P < Q$ an, sodafs $\frac{P-1}{2} \cdot Q = \frac{Q-1}{2} \cdot P - \frac{Q-P}{2}$ $< \frac{Q-1}{2} \cdot P$ ist, so sind die Quotienten α_h sämtlich kleiner als $\frac{Q-1}{2}$, und sind zudem unter einander verschieden, da der auf α_h folgende Quotient α_{h+1} wegen der Gleichung

$$(h+1)\,Q = \alpha_{h+1}\,P + \varrho_{h+1} = \alpha_h\,P + (Q + \varrho_h)$$

mindestens um 1 gröfser sein mufs als α_h. Stellen wir nun der Zahlenreihe (191) die andere:

$$(194)\qquad 1 \cdot P,\ 2 \cdot P,\ 3 \cdot P, \ldots \frac{Q-1}{2} \cdot P$$

und den jener Reihe entsprechenden Gleichungen (193) die folgenden:

$$(195)\qquad \begin{gathered} k\,P = a_k \cdot Q + r_k \\ \left(\text{für } k = 1, 2, 3, \cdots \frac{Q-1}{2}\right), \end{gathered}$$

in denen r_k wieder den kleinsten positiven Rest (mod. Q) bedeutet, gegenüber. Bedeuten v', w' für P, Q dasselbe, wie v, w für Q, P, so besteht die mit (192) analoge Gleichung

$$(196) \qquad \left(\frac{P}{Q}\right) = (-1)^{v'+w'}.$$

Hier nehmen die Quotienten a_k, da $\frac{Q-1}{2} \cdot P = \frac{P-1}{2} \cdot Q + \frac{Q-P}{2}$ und der Rest $\frac{Q-P}{2}$ positiv und $< Q$, mithin $a_{\frac{Q-1}{2}} = \frac{P-1}{2}$ ist, und da sie wegen

$$(197) \qquad (k+1)\,P = a_{k+1}\,Q + r_{k+1} = a_k\,Q + (P + r_k)$$

höchstens immer um eine Einheit wachsen können, sämtliche Werte $1, 2, 3, \cdots \frac{P-1}{2}$ an. Die Reste r_k lassen sich aber in zwei Arten R', R'' unterscheiden: die erste Art umfaſst diejenigen von ihnen, welche sich von dem darauf folgenden Reste um eine ungerade, die zweite Art diejenigen, die sich von dem darauf folgenden Reste um eine gerade Zahl unterscheiden. Der letztere Fall wird sich ereignen, so oft r_k, r_{k+1} gleichartige Zahlen, also, weil kP, $(k+1)\,P$ ungleichartig sind, so oft a_k, a_{k+1} ungleichartige Zahlen sind d. h. $a_{k+1} = 1 + a_k$ ist; er ereignet sich also $\frac{P-1}{2}$ Mal.

Sei nun zuerst Q von der Form $4z+1$, also $\frac{Q-1}{2}$ gerade. Alsdann lassen sich die Reste r_k vom ersten an gerechnet in $\frac{Q-1}{4}$ Paare teilen. Steht an der ersten Stelle eines solchen Paares d. h. an einer ungeraden Stelle der Reihe (194) ein Rest r_k der Art R', so steht an der folgenden geraden Stelle ein mit r_k ungleichartiger Rest, demnach liefert dieses Paar zur Summe $v' + w'$ den Beitrag Null oder Zwei, jenachden r_k ungerade oder gerade ist; da es aber in der Formel (196) nur auf den Rest von $v' + w'$ (mod. 2) ankommt, kann jenes Paar vernachlässigt werden. Steht dagegen an erster Stelle des Paares d. i. an ungerader Stelle der Reihe (194) ein Rest r_k der zweiten Art R'', so steht an der folgenden geraden Stelle ein mit r_k gleichartiger Rest, und somit liefert der erste oder der zweite dieser Reste zur Summe $v' + w'$ den Beitrag Eins, jenachdem sie gerade resp. ungerade sind. Hieraus folgt, daſs $v' + w'$ (mod. 2) mit der Anzahl dieser letzteren Fälle kongruent sein muſs.

Um sie zu ermitteln, schreibe man die Formel (193), wie folgt:

$$(198) \qquad \alpha_h\,P = (h-1)\,Q + (Q - \varrho_h),$$

wo der Rest $Q - \varrho_h$ positiv und $< Q$ ist. Da, wie gezeigt, $\alpha_h < \frac{Q-1}{2}$ ist, so ist diese Gleichung eine der Formeln (195) und es treten also sämtliche Gleichungen (193), wenn man sie in der angegebenen Weise

umschreibt, unter den Gleichungen (195) auf. Die folgende der letzteren Gleichungen lautet dann

$$(199) \qquad (\alpha_h + 1) P = h Q + (P - \varrho_h)$$

und giebt also einen mit dem vorigen gleichartigen Rest. Da die Anzahl der Gleichungen (193) gleich $\frac{P-1}{2}$ d. i. gleich der Anzahl der Reste der zweiten Art R'' ist, so liefern also die Gleichungen (198) die sämtlichen Reste dieser Art, und ein solcher steht folglich in der Reihe (194) an gerader oder an ungerader Stelle, jenachdem α_h gerade oder ungerade ist. Die zu ermittelnde Anzahl beträgt daher u und folglich ist

$$v' + w' \equiv u \pmod{2}$$

und

$$\left(\frac{P}{Q}\right) = (-1)^u = \left(\frac{Q}{P}\right).$$

Ist aber zweitens Q von der Form $4z + 3$ also $\frac{Q-1}{2}$ ungerade, so lassen sich die sämtlichen Reste r_k, vom ersten an gerechnet, in $\frac{Q-3}{4}$ Paare teilen, zu denen noch ein einzelner letzter Rest $\frac{Q-P}{2}$ hinzutritt. Bezüglich jener Paare bleiben die bisherigen Betrachtungen ungeändert, und es wird daher $v' + w' \equiv u$ oder $v' + w' \equiv u + 1 \pmod{2}$ sein, jenachdem der letzte Rest, welcher an ungerader Stelle der Reihe (194) steht, ungerade oder gerade d. h. jenachdem P von der Form $4z + 1$ oder von der Form $4z + 3$ ist. Im erstern Falle ist folglich

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right),$$

im letztern Falle

$$\left(\frac{P}{Q}\right) = -\left(\frac{Q}{P}\right).$$

Alle diese Fälle vereinigen sich in der Formel des Reziprozitätsgesetzes.

Der hiermit gelieferte neue Beweis des letztern vereinfacht sich erheblich, wenn man statt der Reste in den Gleichungen (193), (195) die Quotienten α_h, a_k in Betracht zieht. Es ist schon bemerkt, dafs

$$\left(\frac{Q}{P}\right) = (-1)^u$$

ist, wenn u die Anzahl der ungeraden Quotienten α_h bedeutet; ebenso wird

$$\left(\frac{P}{Q}\right) = (-1)^{u'},$$

wenn u' die Anzahl der ungeraden Quotienten a_k bezeichnet. Nun ist (198) die α_h^{te} der Gleichungen (195) und ihr Quotient ist $h - 1$,

während in (199) d. i. in der folgenden dieser Gleichungen der Quotient schon h ist; die α_h^{te} der Gleichungen (195) ist also die letzte mit dem Quotienten $h-1$, ebenso die α_{h+1}^{te} die letzte mit dem Quotienten h, und somit tritt in diesen Gleichungen der Quotient h genau $\alpha_{h+1}-\alpha_h$ Mal auf. Da hiernach die $\alpha_{\frac{P-1}{2}}^{\text{te}}$ Gleichung noch den Quotienten $\frac{P-3}{2}$, von der folgenden an aber bis zur letzten Gleichung, deren Nummer $\frac{Q-1}{2}$ ist, jede den Quotienten $\frac{P-1}{2}$ haben mufs, welcher dieser entspricht, so wird der letztere genau $\frac{Q-1}{2}-\alpha_{\frac{P-1}{2}}$ Mal auftreten. Beschränkt man sich nur auf die ungeraden Quotienten α_k, so findet sich hieraus für deren Anzahl u' folgende Bestimmung:

wenn $\frac{P-1}{2}$ gerade ist:

$$u' = \alpha_2-\alpha_1+\alpha_4-\alpha_3+\cdots+\alpha_{\frac{P-1}{2}}-\alpha_{\frac{P-3}{2}}$$

d. i.

$$u' \equiv \alpha_1+\alpha_2+\cdots\alpha_{\frac{P-1}{2}} \pmod{2}$$

oder, indem man hier die geraden α_h unterdrückt und die ungeraden durch Eins ersetzt,

$$u' \equiv u \pmod{2};$$

wenn dagegen $\frac{P-1}{2}$ ungerade ist:

$$u' = \alpha_2-\alpha_1+\alpha_4-\alpha_3+\cdots+\alpha_{\frac{P-3}{2}}-\alpha_{\frac{P-5}{2}}+\frac{Q-1}{2}-\alpha_{\frac{P-1}{2}}$$

d. i.

$$u' \equiv \alpha_1+\alpha_2+\cdots+\alpha_{\frac{P-1}{2}}+\frac{Q-1}{2} \pmod{2}$$

und daher

$$u' \equiv u \text{ oder } u' \equiv u+1 \pmod{2},$$

jenachdem $\frac{Q-1}{2}$ gerade oder ungerade ist.

Aus diesen Resultaten ergiebt sich aber wieder sogleich das Reziprozitätsgesetz.

Unter allen auf das Gaufssche Lemma gegründeten Beweisen will mir dieser Langesche Beweis, namentlich in seiner letzten einfacheren Gestalt, als der ursprünglichste oder natürlichste erscheinen, insofern er, in den Gleichungen (193), (195) auf die Grundformel der Zahlentheorie zurückgreifend, die reziproke Beziehung zwischen den beiden Zahlenreihen (191) und (194) lediglich aus dem Umstande entwickelt, dafs die h^{te} der Gleichungen (193) als die α_h^{te} der Gleichungen (195) auftreten mufs. —

21. Wir wenden uns nunmehr zu den beiden Beweisen von Chr. Zeller und von Petersen (Zeller, *Berl. Monatsber.* 1872,

p. 846; Petersen, *Americ. Journ. of math.* 2, 1879, p. 285 oder Zeuthen, *Tidskr.* 1879, p. 86), welche auch auf dem Gaufsschen Lemma, jedoch bei dessen Anwendung auf einem neuen Grundgedanken beruhen, der, wie Kroneckers tiefere Deutung dieser Beweise (*Berl. Sitzungsber.* 1885, p. 383) gelehrt hat, auf die Benutzung zweier weiteren Eigenschaften der Funktion $R(x)$ zurückkommt. Diese sollen daher zuvörderst angemerkt werden.

Sind a, b, c drei beliebige reelle Werte, so folgt aus den Gleichungen

$$R(a) = a - \left[a + \frac{1}{2}\right]$$

$$R(b) = b - \left[b + \frac{1}{2}\right]$$

$$R(c) = c - \left[c + \frac{1}{2}\right],$$

dafs, so oft die Summe $a + b + c$ ganzzahlig ist, dasselbe auch von der Summe $R(a) + R(b) + R(c)$ gilt. Da aber $R(x)$ stets numerisch kleiner als $\frac{1}{2}$ ist, so liegt diese Summe, wenn alle drei Reste $R(a)$, $R(b)$, $R(c)$ negativ sind, zwischen 0 und $-\frac{3}{2}$, wenn sie alle drei positiv sind, zwischen 0 und $+\frac{3}{2}$, andernfalls zwischen $+1$ und -1, und somit hat man den Satz:

Ist die Summe $a + b + c$ ganzzahlig, so ist

$$R(a) + R(b) + R(c) = \begin{cases} 1 \\ 0, \\ -1 \end{cases} \tag{200}$$

jenachdem die drei Reste zugleich positiv, verschiedenen Vorzeichens, oder zugleich negativ sind.

Sind andererseits v, w zwei positive Werte, deren Produkt $vw = 1$ ist, so giebt es unendlich viel Paare ganzer Zahlen h, k von der Art, dafs

$$\frac{R(hw)}{\sqrt{w}} + \frac{R(kv)}{\sqrt{v}} = 0 \tag{201}$$

ist, wo unter den Quadratwurzeln ihre absoluten Werte verstanden sind.

In der That, setzt man $v \overline{\gtrless} 1$ voraus und für die beliebige ganze Zahl h die Gleichung an:

$$hw = k + R(hw),$$

sodafs $k = \left[hw + \frac{1}{2}\right]$ ist, so wird

$$kv = h - vR(hw)$$

d. h., da $v\,R\,(h\,w)$ absolut $< \frac{1}{2}$ ist, $h = \left[k\,v + \frac{1}{2}\right]$ und $R\,(k\,v) = -\,v\,R\,(h\,w)$, aus welcher Gleichung die behauptete Beziehung (201) unmittelbar hervorgeht, wenn sie mit $v\sqrt{w} = \sqrt{v}$ dividiert wird.

Nun seien wieder P, Q zwei positive, ungerade, relativ prime Zahlen und $Q > P$. Die absolut kleinsten Reste der Vielfachen

$$(202)\qquad 1\cdot Q,\ 2\cdot Q,\ 3\cdot Q, \cdots \frac{P-1}{2}\cdot Q\ (\text{mod.}\ P),$$

welche positiv sind, seien β_1, $\beta_2 \ldots \beta_\lambda$, diejenigen, welche negativ sind, seien $-\alpha_1, -\alpha_2, \ldots, -\alpha_\mu$, sodaſs $\lambda + \mu = \frac{P-1}{2}$ ist und, wie schon früher bemerkt, die Zahlen α und β zusammengenommen die ganze Reihe der Zahlen $1, 2, 3, \cdots \frac{P-1}{2}$ erschöpfen. Ebenso seien die absolut kleinsten positiven resp. negativen Reste der Vielfachen

$$(203)\qquad 1\cdot P,\ 2\cdot P,\ 3\cdot P, \cdots \frac{Q-1}{2}\cdot P\ (\text{mod}\ Q)$$

die Zahlen $\delta_1, \delta_2, \cdots \delta_\varrho$ resp. $-\gamma_1, -\gamma_2, \cdots, -\gamma_\nu$, sodaſs $\nu + \varrho = \frac{Q-1}{2}$ ist und die Gesamtheit der Zahlen γ und δ mit der Reihe $1, 2, 3, \cdots \frac{Q-1}{2}$ identisch ist. Da $Q > P$ vorausgesetzt und jede Zahl $\gamma < \frac{Q}{2}$ ist, so lassen sich diese Zahlen in zwei Arten γ', γ'' unterscheiden, von denen die ersteren $< \frac{P}{2}$, die anderen zwischen $\frac{P}{2}$ und $\frac{Q}{2}$ enthalten sind.

Nun zeigt die fundamentale Kongruenz (78), wenn sie in Form einer Gleichung:

$$(204)\qquad h\,Q = k\,P + r$$

geschrieben wird, wo $r = \pm h'$ absolut kleiner als $\frac{P}{2}$ ist, weil dann aus ihr die andere Gleichung

$$(205)\qquad k\,P = h\,Q - r$$

hervorgeht, daſs jeder negative Rest (mod. P) ein positiver Rest (mod. Q), d. h. jede der Zahlen α eine der Zahlen δ, und ebenso, daſs jede der Zahlen β eine der Zahlen γ, genauer, da r absolut kleiner als $\frac{P}{2}$ ist, eine der Zahlen γ' ist. Das letztere gilt offenbar auch umgekehrt, und da die Zahlen α, β zusammengenommen die Reihe $1, 2, 3, \cdots \frac{P-1}{2}$ ausmachen, so gilt daher das Gleiche für die Gesamtheit der Zahlen α und γ'.

Den Gleichungen (204) und (205) entsprechen die beiden, welche folgen:

$$R\left(\frac{h\,Q}{P}\right) = \frac{r}{P},\ R\left(\frac{k\,P}{Q}\right) = \frac{-r}{Q}$$

und aus ihnen geht die andere

$$P \cdot R\left(\frac{hQ}{P}\right) + Q \cdot R\left(\frac{kP}{Q}\right) = 0 \tag{206}$$

hervor, die nichts anderes ist als die Gleichung (201) für $v = \frac{P}{Q}$, $w = \frac{Q}{P}$. Durch diese Beziehung, die jeder der Gleichungen (204), (205) substituiert werden kann, wird jeder der Zahlen $h = 1, 2, 3, \cdots \frac{P-1}{2}$ eine bestimmte der Zahlen $k = 1, 2, 3, \cdots \frac{Q-1}{2}$ zugeordnet in der Weise, daſs die Reste $R\left(\frac{hQ}{P}\right)$, $R\left(\frac{kP}{Q}\right)$ entgegengesetzte Vorzeichen haben und der letztere von ihnen absolut kleiner ist als $\frac{P}{2Q}$. Demnach beträgt die Anzahl der negativen Reste $R\left(\frac{hQ}{P}\right)$ und die Anzahl derjenigen negativen Reste $R\left(\frac{kP}{Q}\right)$, welche absolut kleiner sind als $\frac{P}{2Q}$, d. i. die Anzahl der Zahlen α und γ', übereinstimmend mit dem zuvor Bewiesenen, $\frac{P-1}{2}$.

Sei nun aber $R\left(\frac{kP}{Q}\right)$ ein negativer Rest, der absolut gröſser ist als $\frac{P}{2Q}$, sodaſs man setzen darf

$$\frac{kP}{Q} = m - \varrho,$$

wo m eine ganze Zahl und $\varrho > \frac{P}{2Q}$ aber $< \frac{1}{2}$ ist, so bestimme man die Zahl k' durch die Bedingung

$$k + k' = \frac{Q-1}{2}; \tag{207}$$

dann wird

$$\frac{k'P}{Q} = \frac{P}{2} - \frac{P}{2Q} - m + \varrho$$

$$\frac{k'P}{Q} + \frac{1}{2} = \frac{P+1}{2} - m + \left(\varrho - \frac{P}{2Q}\right),$$

worin $\varrho - \frac{P}{2Q}$ ein positiver Wert $< \frac{1}{2}$ ist; mithin findet sich

$$\left[\frac{k'P}{Q} + \frac{1}{2}\right] = \frac{P+1}{2} - m$$

folglich

$$R\left(\frac{k'P}{Q}\right) = -\left(\frac{1}{2} - \left(\varrho - \frac{P}{2Q}\right)\right)$$

d. h. negativ und absolut $> \frac{P}{2Q}$, wie $R\left(\frac{kP}{Q}\right)$. Wir bemerken, daſs man die letzte Gleichung folgendermaſsen schreiben kann:

$$R\left(\frac{kP}{Q}\right) + R\left(\frac{k'P}{Q}\right) + \frac{P}{2Q} - \frac{1}{2} = -1;$$

setzt man hier

$$a = \frac{kP}{Q},\ b = \frac{k'P}{Q},\ c = \frac{P}{2Q} + \frac{1}{2},$$

wo dann $a + b + c = \frac{P+1}{2}$ ganzzahlig und $R(c) = \frac{P}{2Q} - \frac{1}{2}$ wird, so nimmt sie die Gestalt

$$R(a) + R(b) + R(c) = -1$$

an, ganz übereinstimmend mit dem in (200) ausgesprochenen Satze.

Aus dem Gesagten geht nun hervor, dafs jedem Werte von k, welchem ein negativer Wert $R\left(\frac{kP}{Q}\right)$ von gröfserem Absolutwerte als $\frac{P}{2Q}$ zugehört, durch die Formel (207) ein zweiter Wert k' zugeordnet ist, dem gleichfalls ein negativer Wert $R\left(\frac{k'P}{Q}\right)$ von gröfserem Absolutwerte als $\frac{P}{2Q}$ entspricht. Die Anzahl derartiger negativer Werte d. i. offenbar die Anzahl der Zahlen γ'' wird also gerade sein, wenn die zwei sich entsprechenden Zahlen k, k' immer verschieden von einander sind. Der Fall, dafs sie gleich sind, kann sich nur ereignen, wenn $\frac{Q-1}{2}$ gerade ist, und er ereignet sich dann für $k = \frac{Q-1}{4}$, falls für diesen Wert $R\left(\frac{kP}{Q}\right)$ negativ und absolut gröfser als $\frac{P}{2Q}$ ist; nun ist aber den Gleichungen

$$\frac{Q-1}{4} \cdot P = \frac{P-1}{4} \cdot Q + \frac{Q-P}{4},$$

$$\frac{Q-1}{4} \cdot P = \frac{P+1}{4} \cdot Q - \frac{Q+P}{4}$$

zufolge $R\left(\frac{Q-1}{4} \cdot \frac{P}{Q}\right)$ positiv, wenn P von der Form $4z+1$, dagegen negativ und absolut gröfser als $\frac{P}{2Q}$, wenn P von der Form $4z+3$ ist; in diesem letztern Falle also, und nur in ihm, würde die Anzahl jener negativen Werte $R\left(\frac{kP}{Q}\right)$ oder die der Zahlen γ'' ungerade sein. Nennt man diese Anzahl allgemein C, so ist die gesamte Anzahl aller negativen Werte $R\left(\frac{hQ}{P}\right)$ und $R\left(\frac{kP}{Q}\right)$ gleich $\frac{P-1}{2} + C$ und wird also

gerade sein: wenn $\frac{P-1}{2}$ gerade, oder wenn $\frac{P-1}{2}$ ungerade, zugleich aber $\frac{Q-1}{2}$ gerade ist, dagegen

ungerade: wenn $\frac{P-1}{2}$, $\frac{Q-1}{2}$ zugleich ungerade sind. Dies ist aber genau, was das Reziprozitätsgesetz aussagt, wenn es in der zweiten der in Nr. 10 angegebenen Formulierungen gefafst wird.

22. Den gleichen Grundgedanken, wie dieser Zellersche Beweis, der zuerst aus allen negativen Resten $R\left(\frac{kP}{Q}\right)$ diejenigen heraushebt, welche mit Resten $R\left(\frac{hQ}{P}\right)$ durch die Gleichung (206) verbunden sind, und dann die übrigen paarweise verknüpft, führt auch derjenige von Petersen durch und er ist daher ebenfalls im tiefsten Grunde, wie man bei Kronecker a. a. O. nachsehen mag, auf die beiden Eigenschaften (200), (201) der Funktion $R(x)$ begründet. Aber er nimmt wieder das Gaufssche Lemma in einer besonderen Fassung zum Ausgangspunkte, und wir wollen, während wir dem Leser überlassen, die Durchführung des Beweises im Einzelnen in Petersen's Arbeit zu verfolgen, wenigstens diese neue Auffassung des Gaufsschen Lemma sowie den Zusammenhang, in welchem der Beweis von Petersen mit demjenigen von Zeller steht, hier kurz noch erörtern.

Nach (189) ist

$$\left(\frac{Q}{P}\right) = (-1)^u, \tag{208}$$

wenn u die Anzahl der ungeraden kleinsten positiven Reste in der Reihe der Zahlen

$$2Q,\ 4Q,\ 6Q,\ \ldots\ (P-1)\,Q \pmod{P}$$

bedeutet. Da diese Zahlen, negativ genommen, in umgekehrter Reihenfolge den ungeraden Vielfachen

$$1Q,\ 3Q,\ 5Q,\ \ldots\ (P-2)\,Q \pmod{P} \tag{209}$$

kongruent sind, so bedeutet u offenbar auch die Anzahl derjenigen dieser Vielfachen, deren Rest, wenn er $< P$ und ungerade gewählt wird, negativ ist. Wir nehmen hier die Gelegenheit wahr, zunächst zu zeigen, dafs $u = \mu(Q, P)$ ist. Ist nämlich

$$(2i-1)\,Q \equiv \pm(2i'-1) \pmod{P}, \tag{210}$$

so folgt

$$(P-2i+1)\,Q \equiv \pm(P-2i'+1) \pmod{P}$$

also, wenn man $P-2i+1 = 2h$, $P-2i'+1 = 2h'$ setzt, wo dann h, h' positiv und kleiner als $\frac{P}{2}$ sein werden, auch die Kongruenz

$$hQ \equiv \pm h' \pmod{P}, \tag{211}$$

und aus dieser umgekehrt die ursprüngliche. Ebensoviel Vielfache der Reihe (209) geben also einen negativen ungeraden Rest $< P$, als es in der Reihe

$$1\cdot Q,\ 2\cdot Q,\ 3\cdot Q,\ \cdots\ \frac{P-1}{2}\cdot Q \tag{212}$$

Vielfache giebt, deren absolut kleinster Rest negativ ist. Mithin ist $u = \mu(Q, P)$.

Aus der vorstehenden Betrachtung folgt auch, dafs man die Kongruenz (210) durch die andere:

$$(213) \qquad (2i-1)\,Q \equiv (2i'-1)\cdot \operatorname{sgn.} R\left(\frac{hQ}{P}\right) \pmod{P}$$

ersetzen darf. Nun ist

$$\operatorname{sgn.} R\left(\frac{hQ}{P}\right) = (-1)^{\left[\frac{2hQ}{P}\right]} = (-1)^{\left[\frac{(P-2h)\,Q}{P}\right]}.$$

Wenn aber $2i-1 < \frac{P}{2}$ ist, so ist $P-2h$ eine ungerade Zahl $< \frac{P}{2}$; für $2i-1 > \frac{P}{2}$ dagegen ist $2h$ eine gerade Zahl $< \frac{P}{2}\cdot$ Bildet man daher die Kongruenz (213) für alle Zahlen $2i-1 = 1, 3, 5, \cdots (P-2)$ und wählt dabei rechts für $\operatorname{sgn.} R\left(\frac{hQ}{P}\right)$ den zweiten Ausdruck, solange $2i-1 < \frac{P}{2}$ bleibt, für die ferneren Werte von $2i-1$ dagegen den ersten, so erhält man rechts im Exponenten von -1 sämtliche Vielfachen (212) und findet durch Multiplikation der erhaltenen Kongruenzen die folgende:

$$\prod (2i-1)\cdot Q^{\frac{P-1}{2}} \equiv \prod (2i'-1)\cdot (-1)^{\sum\limits_{h=1}^{\frac{P-1}{2}}\left[\frac{hQ}{P}\right]} \pmod{P}.$$

Da aber, wenn $2i-1$ die Reihe $1, 3, 5 \ldots (P-2)$ durchläuft, die Zahl h' zugleich mit der Zahl h alle Werte $1, 2, 3, \cdots \frac{P-1}{2}$ annimmt, so durchläuft auch $2i'-1$ die Reihe der Zahlen $1, 3, 5, \ldots (P-2)$ in gewisser Folge, daher ist

$$\prod (2i-1) = \prod (2i'-1) = 1\cdot 3\cdot 5\cdots (P-2).$$

In dem speziellen Falle, wo P, Q zwei verschiedene ungerade Primzahlen p, q sind, in welchem Falle $q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}$ ist, darf man daher in obiger Kongruenz den gleichen Faktor beiderseits unterdrücken und erhält die auf diesen Fall bezügliche Gaufssche Formel

$$\left(\frac{q}{p}\right) = (-1)^{\sum\limits_{h=1}^{\frac{p-1}{2}}\left[\frac{hq}{p}\right]} = \prod_{h=1,\ k=1}^{\frac{p-1}{2},\ \frac{q-1}{2}} \left(\frac{k}{q} - \frac{h}{p}\right),$$

welche dann wieder, wie in Nr. 14, zum einfachen, aber mittelbar so auch zum verallgemeinerten Reziprozitätsgesetze führt.

Nach dieser Zwischenbetrachtung, welche eine neue Modifikation der Kroneckerschen Beweise des Reziprozitätsgesetzes bildet (s. Kronecker, *Berl. Sitzgsber.* 1885, p. 117), wenden wir uns wieder zu Petersen zurück.

Bezeichnet u' die Anzahl derjenigen Vielfachen

$$(214) \qquad 1 \cdot P,\ 3 \cdot P,\ 5 \cdot P, \cdots (Q-2)\, P,$$

deren Rest (mod. Q), wenn er ungerade und $< Q$ gewählt wird, negativ ist, so hat man analog mit (208)

$$(215) \qquad \left(\frac{P}{Q}\right) = (-1)^{u'}.$$

Nun entspricht jedem der Vielfachen (209) eine Gleichung von der Form

$$(216) \qquad (2i-1)\, Q = 2gP + r,$$

in welcher $r = \pm(2i'-1)$ eine ungerade Zahl und absolut genommen $< P$ ist. Desgleichen giebt jedes der Vielfachen (214) eine Gleichung von der Form

$$(217) \qquad (2i_1 - 1)\, P = 2g_1 Q + r_1,$$

wo r_1 eine ungerade Zahl und numerisch $< Q$ ist. Wir setzen wieder $Q > P$ voraus. Schreibt man die Gleichung (216), wie folgt:

$$(Q-2g)\, P = (P-2i+1)\, Q + r,$$

so geht sie, da r absolut $< P$ also auch $< Q$ ist, in eine derjenigen Gleichungen (217) über, deren Rest r_1 absolut kleiner als P ist. Man sieht daher, daſs jedem Vielfachen (209) mit negativem ungeraden Reste $< P$ ein Vielfaches (214) zugehört, dessen ungerader Rest ebenfalls negativ und $< P$ ist, sowie auch umgekehrt. Demnach wird die Anzahl aller Vielfachen (209) und (214), deren ungerader Rest negativ ist, d. h. die Zahl $u + u'$, gerade oder ungerade und demnach $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = +1$ oder -1 sein, jenachdem die Anzahl derjenigen Vielfachen (214), deren ungerader Rest zwischen $-P$ und $-Q$ liegt, gerade oder ungerade ist. Man sieht, wie der Gedankengang des Petersenschen Beweises demjenigen des Zellerschen völlig parallel läuft. Indem wir nun den Leser bezüglich der Entscheidung über die letztbezeichnete Alternative, die zum Reziprozitätsgesetze führt, auf die Arbeit von Petersen verweisen, bemerken wir nur noch zum Schlusse, daſs die Gleichungen (216) nichts anderes sind, als eine andere Gestalt der Gleichungen (204) im Zellerschen Beweise, wie unmittelbar erhellt, wenn man für $2i-1$, $2i'-1$ die korrespondierenden Zahlen h, h' einführt; denn so geht aus ihr die folgende Gleichung

$$hQ = \frac{Q \mp 1 - 2g}{2}\, P \pm h'$$

hervor, d. i., indem man $k = \frac{Q \mp 1}{2} - g$ setzt, die Gleichung (204). Dadurch ist zur Genüge der enge innere Zusammenhang beider Beweise gekennzeichnet.

Wir wollen aber noch in Erinnerung bringen, dafs die Formel (188) für jede positive zu P prime Zahl z bewiesen ist, dafs mithin die Formel (189) auch bestehen bleibt, wenn Q nicht ungerade ist. Somit darf man z. B. $Q = 2$ wählen und erhält dann

$$\left(\frac{2}{P}\right) = (-1)^u, \tag{218}$$

wenn u die Anzahl derjenigen Vielfachen

$$1 \cdot 2,\ 3 \cdot 2,\ 5 \cdot 2, \cdots (P-2) \cdot 2 \tag{219}$$

bedeutet, deren Rest (mod. P), wenn er ungerade und $< P$ gewählt wird, negativ ist, sodafs gesetzt werden kann:

$$2u' = mP - u'',$$

wo u', u'' ungerade Zahlen $< P$ und auch m eine ungerade Zahl bezeichnet.

Aus dieser Gleichung folgt aber die andere:

$$2(P - 1 - u') = (2 - m)P + (u'' - 2),$$

in welcher der Rest positiv ist, es sei denn $u'' = 1$ d. h. $2u' = mP - 1$, ein Fall, der sich nur ereignet, wenn $2u' = P - 1$ d. h. $u' = \frac{P-1}{2}$ und demnach P von der Form $4z + 3$ ist. Somit findet sich, dafs, wenn P von der Form $4z + 1$ ist, jedem Vielfachen (219) mit negativem ungeraden Reste $< P$ ein solches mit positivem Reste zugehört, und umgekehrt, die Anzahl u der erstern ist also gleich $\frac{P-1}{4}$. Wenn dagegen P von der Form $4z + 3$ ist, so giebt das Vielfache $\frac{P-1}{2} \cdot 2$ einen negativen ungeraden Rest $< P$, von den übrigen $\frac{P-3}{2}$ Vielfachen ist aber wieder stets eins mit negativem ungeraden Reste $< P$ einem solchen mit positivem Reste verbunden, und somit beträgt in diesem Falle die Anzahl u aller derjenigen Vielfachen (219), welche negative ungerade Reste $< P$ haben, $1 + \frac{P-3}{4} = \frac{P+1}{4}$. Der Formel (218) zufolge ist daher

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P-1}{4}} \quad \text{oder} \quad (-1)^{\frac{P+1}{4}},$$

jenachdem $\frac{P-1}{2}$ gerade oder ungerade ist, was zu der Formel (50) oder (51) wieder zurückführt und so einen neuen Beweis des zweiten Ergänzungssatzes ausmacht.

23. Ohne das Gaufssche Lemma als ihre Grundlage zu verleugnen, stehen doch mehrere andere Beweise in nur loserem Zusammenhange mit den bisher dargestellten. Wir skizzieren von ihnen zunächst den Beweis von **Bouniakowsky** (*Bull. de St. Pét.* 22, 1876), welcher zu dem an erster Stelle mitgeteilten Buscheschen Beweise ein näheres Verhältnis hat.

Seien a, r positive ungerade Zahlen ohne gemeinsamen Teiler und $p = 2an + r$ eine ungerade Primzahl. Mittels einer durch die Zahlen a, r fest bestimmten Verteilung der Zahlen $1, 2, 3, \cdots \frac{p-1}{2}$ in eine Reihe von Abschnitten und der ihnen entsprechenden Zerfällung des Produkts $1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}$ in Teilprodukte gelingt es Bouniakowsky zu zeigen, dafs

$$(220) \qquad \left(\frac{a}{p}\right) = (-1)^{\frac{a-1}{2}n+m}$$

gesetzt werden kann, wo m eine nur von a, r abhängige Zahl ist. Ohne diesen Teil der Bouniakowskyschen Betrachtung hier zu reproduzieren, soll vielmehr gezeigt werden, dafs diese Gleichung sich leicht aus den bei jenem Buscheschen Beweise gelieferten Formeln ableiten läfst. In der That besteht für die Zahl $m = \mu(a, r)$ nach (114) die Kongruenz

$$\mu(a, r) \equiv \psi(a, r) \equiv \sum_{h=1}^{\frac{r-1}{2}} \left[\frac{ha}{r}\right] \pmod{2};$$

nach (175) findet sich also

$$\mu(a, r + 2na) \equiv \mu(a, r) + n \cdot \left(\frac{a-1}{2}\right)^2 \pmod{2}$$

d. i., wenn P irgend eine durch die Gleichung $P = 2an + r$ definierte Zahl ist,

$$\mu(a, P) \equiv m + n \cdot \frac{a-1}{2} \pmod{2}$$

folglich

$$(221) \qquad \left(\frac{a}{P}\right) = (-1)^{m + n \cdot \frac{a-1}{2}},$$

sodafs die Formel (220) sogar in gröfserer Allgemeinheit bestätigt ist.

Sind nun wieder P, Q zwei positive ungerade relativ prime Zahlen und $P > Q$, so wird $P - Q$ eine positive gerade Zahl, also

$$(222) \qquad P - Q = 2^\alpha \cdot a$$

gesetzt werden können, wo $\alpha \gtreqless 1$, a ungerade ist, und da somit $P, Q \pmod{2a}$ kongruent sind, läfst sich

$$P = 2an + r, \qquad Q = 2an' + r$$

setzen, wo offenbar der Rest r eine positive ungerade Zahl ohne gemeinsamen Teiler mit a ist, da sonst P, Q nicht teilerfremd wären. In Gemäfsheit der Formel (221) darf man daher setzen

$$\left(\frac{a}{P}\right) = (-1)^{m+n\cdot\frac{a-1}{2}}, \quad \left(\frac{a}{Q}\right) = (-1)^{m+n'\cdot\frac{a-1}{2}}$$

mithin

$$\left(\frac{a}{P}\right)\left(\frac{a}{Q}\right) = (-1)^{(n+n')\cdot\frac{a-1}{2}}.$$

Aus (222) aber folgen die Gleichungen

$$\left(\frac{P}{Q}\right) = \left(\frac{2^{\alpha}a}{Q}\right), \quad \left(\frac{Q}{P}\right) = \left(\frac{-2^{\alpha}a}{P}\right)$$

also mit Rücksicht auf die vorstehende Formel und auf die beiden Ergänzungssätze

$$(223) \qquad \left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}+\alpha\left(\frac{P^2-1}{8}+\frac{Q^2-1}{8}\right)+(n+n')\cdot\frac{a-1}{2}}.$$

Ist nun erstens $\alpha \gtreqless 3$, so folgt aus (222)

$$P \equiv Q \text{ (mod. 8)}, \quad n - n' \equiv 0 \text{ (mod. 4)},$$

also

$$\frac{P^2-1}{8} + \frac{Q^2-1}{8} \equiv 0, \quad n + n' \equiv 0 \text{ (mod. 2)}$$

und demgemäfs

$$(224) \qquad \left(\frac{P}{Q}\right)\cdot\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}}$$

d. h. gleich $+1$ oder -1, jenachdem P, Q beide von der Form $4z+1$ oder beide von der Form $4z+3$ sind.

Ist zweitens $\alpha = 2$, so folgt aus (222)

$$P \equiv Q \text{ (mod. 4)}, \quad n - n' \equiv 0 \text{ (mod. 2)}$$

also wieder die Formel (224) und die gleiche Folgerung.

Ist drittens $\alpha = 1$, so folgt $P - Q \equiv 2$ (mod. 4), ferner $n = n' + 1$ also $n + n' \equiv 1$ (mod. 2) und daher

$$\left(\frac{P}{Q}\right)\cdot\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}+\frac{a-1}{2}+\frac{P^2-1}{8}+\frac{Q^2-1}{8}}.$$

Setzt man aber die gerade Zahl $P - a = a + Q$ gleich $2b$, so findet man ohne Schwierigkeit

$$\frac{P^2-1}{8} + \frac{Q^2-1}{8} \equiv b \text{ (mod. 2)}$$

also gerade oder ungerade, jenachdem b oder $\frac{P-1}{2} + \frac{a-1}{2}$ gerade oder ungerade ist; man findet also in diesem Falle d. h., wenn P, Q (mod. 4) verschiedene Form haben,

$$\left(\frac{P}{Q}\right)\cdot\left(\frac{Q}{P}\right) = 1.$$

Diese verschiedenen Resultate fassen sich aber zusammen in der Formel des Reziprozitätsgesetzes:

$$\left(\frac{P}{Q}\right)\cdot\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

Mit diesem Beweise von Bouniakowsky hat der erste derjenigen Beweise, welche **H. Schmidt** (*Journ. f. Math.* 111, 1893, p. 107) gegeben hat, mancherlei Ähnlichkeit. Zunächst in dem Umstande, dafs er die Differenz der beiden Zahlen P, Q:

$$P-Q=2n, \tag{225}$$

einführt und das Reziprozitätsgesetz mittelbar aus den Werten von $\left(\frac{n}{P}\right), \left(\frac{n}{Q}\right)$ gewinnt. Hierzu betrachtet er die Reste der Vielfachen

$$1n,\ 2n,\ 3n,\ \cdots \frac{P-1}{2}n \pmod{P}, \tag{226}$$

sowie diejenigen der Vielfachen

$$1n,\ 2n,\ 3n,\ \cdots \frac{Q-1}{2}n \pmod{Q}, \tag{227}$$

die er — wieder ähnlich wie Bouniakowsky — in Abschnitte teilt. Da nämlich $n=\frac{P-Q}{2}<\frac{P}{2}$, so beginnt die Reihe (226) mit Gliedern $<\frac{P}{2}$, denen Glieder $>\frac{P}{2}$ folgen, bis die Glieder $>P$ werden; die Reste derselben werden dann wieder zunächst $<\frac{P}{2}$ sein, allmählich $>\frac{P}{2}$ werden, bis die Glieder $>2P$ werden, u. s. w. So erkennt man, indem man für ein gerades n

$$\frac{P-1}{2}n=P\cdot\left(\frac{n}{2}-1\right)+P-\frac{n}{2}$$

setzt, wo $P-\frac{n}{2}>\frac{P}{2}$, für ein ungerades n

$$\frac{P-1}{2}n=P\cdot\frac{n-1}{2}+\frac{P-n}{2},$$

wo $\frac{P-n}{2}<\frac{P}{2}$ ist, dafs im ersteren Falle $\frac{n}{2}$ Abschnitte vorhanden sind, in denen auf Reste, welche $<\frac{P}{2}$ sind, solche folgen, die $>\frac{P}{2}$ sind, während im zweiten Falle $\frac{n-1}{2}$ solche Abschnitte vorhanden sind, auf deren letzten noch ein Abschnitt folgt, dem nur Reste $<\frac{P}{2}$ zugehören. In dem besonderen Falle, wo $P=Q+2$ also $n=1$ ist, fallen die ersteren $\frac{n-1}{2}$ Abschnitte aus und ist nur der letztbezeichnete mit lauter Resten $<\frac{P}{2}$ vorhanden.

Ist nun

$$(k+1)n, \cdots (k+k')n, \quad (k+k'+1)n, \cdots (k+k'')n$$

ein solcher Abschnitt und hP, $(h+1)P$ die Vielfachen von P, zwischen denen er liegt, und ist $(k+k')n$ das letzte Glied, welches $< \left(h+\frac{1}{2}\right) P$ ist, so erkennt man aus (225) sogleich, dafs die Vielfachen

$$(k+1-2h)n, \cdots (k+k'-2h-1)n, \quad (k+k'-2h)n, \cdots (k+k''-2h-2)n$$

diejenigen Vielfachen der Reihe (227) sind, welche zwischen hQ und $(h+1)Q$ enthalten sind, und dafs $(k+k'-2h-1)n$ das letzte von ihnen $< \left(h+\frac{1}{2}\right) Q$ ist. Mit anderen Worten: die Vielfachen (227) lassen sich in ebensoviel Abschnitte zerlegen, deren jeder aber (im Falle eines ungeraden n von dem letzten abgesehen, der nur Reste $< \frac{Q}{2}$ ergiebt) zwei Glieder — in der Mitte — nämlich ein Glied mit einem Reste $< \frac{Q}{2}$ und ein solches mit einem Reste $> \frac{Q}{2}$ weniger enthält, als die früheren Abschnitte. Nennt man demnach A, B die Anzahl der Reste $> \frac{P}{2}$ resp. $> \frac{Q}{2}$ in den beiden Reihen (226), (227), so ergiebt sich, wenn n gerade ist:

$$A - B = \frac{n}{2},$$

wenn n ungerade ist:

$$A - B = \frac{n-1}{2},$$

mithin allgemein

$$A + B \equiv A - B \equiv \frac{n(n-1)}{2} \pmod{2}.$$

Da aber dem verallgemeinerten Gaufsschen Lemma zufolge

$$\left(\frac{n}{P}\right) = (-1)^A, \quad \left(\frac{n}{Q}\right) = (-1)^B$$

ist, so findet sich

$$\left(\frac{n}{P}\right) \cdot \left(\frac{n}{Q}\right) = (-1)^{\frac{n(n-1)}{2}}$$

also

$$\left(\frac{2n}{P}\right) \cdot \left(\frac{2n}{Q}\right) = (-1)^{\frac{n(n-1)}{2} + \frac{P^2-1}{8} + \frac{Q^2-1}{8}}.$$

Andererseits folgt aus (225)

$$\left(\frac{2n}{P}\right) \cdot \left(\frac{2n}{Q}\right) = \left(\frac{-Q}{P}\right) \cdot \left(\frac{P}{Q}\right)$$

mithin

$$\left(\frac{P}{Q}\right) \cdot \left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} + \frac{P^2-1}{8} + \frac{Q^2-1}{8} + \frac{n(n-1)}{2}},$$

eine Formel, welche entsprechend den Fällen, wo n durch 4 oder nur durch 2 teilbar oder ungerade ist, ganz wie die Formel (223) behandelt werden kann und zum Reziprozitätsgesetze zurückführt.

24. Der zweite Beweis von **Schmidt**, der nur das einfache Reziprozitätsgesetz zwischen zwei positiven ungeraden Primzahlen p, q herleitet, charakterisiert sich als verwandt mit dem fünften Gaufsschen Beweise schon darin, dafs er sich auf die Betrachtung der Zahlenreihe $1, 2, 3, \dots \frac{pq-1}{2}$ gründet.

Man setze

$$\prod = 1 \cdot 2 \cdot 3 \cdots \frac{pq-1}{2}, \tag{228}$$

dagegen P gleich dem Produkte derjenigen Faktoren von $\prod$, welche prim zu $p\,q$ sind, d. h.

$$P = \frac{\Pi}{p \cdot 2p \cdots \frac{q-1}{2} p \cdot q \cdot 2q \cdots \frac{p-1}{2} q}. \tag{229}$$

Ist dann r irgend ein Faktor von P, so giebt es eine Zahl $x < pq$ von der Beschaffenheit, dafs $r \cdot x \equiv 1 \pmod{pq}$ wird; wäre dabei $x > \frac{pq}{2}$, so würde $pq - x$ eine Zahl $< \frac{pq}{2}$ sein, für welche $r(pq - x) \equiv -1 \pmod{pq}$ wäre. Bezeichnet also ε eine passend gewählte Einheit, so giebt es für jeden Faktor r von P einen zweiten Faktor s der Art, dafs $rs \equiv \varepsilon \pmod{pq}$ ist. Hierbei kann r nur dann gleich s sein, wenn

$$r^2 \equiv 1 \quad \text{oder} \quad r^2 \equiv -1 \pmod{pq}$$

ist. Die erste dieser Kongruenzen hat stets vier Wurzeln, von denen zwei kleiner als $\frac{pq}{2}$ sind; eine von diesen ist 1, die andere heifse ϱ. Die zweite Kongruenz dagegen ist nur möglich, wenn beide Primzahlen p, q von der Form $4z+1$ sind, und in diesem Falle hat auch sie vier Wurzeln, von denen zwei kleiner als $\frac{pq}{2}$; heifst eine der letzteren σ, so sind alle vier Wurzeln

$$\sigma,\ pq - \sigma,\ \sigma',\ pq - \sigma',$$

wenn σ' den kleinsten positiven Rest von $\varrho\sigma \pmod{pq}$ bedeutet; also sind diejenigen von ihnen, welche $< \frac{pq}{2}$ sind, entweder σ und σ' oder σ und $pq - \sigma'$. Hieraus folgt, dafs, wenn beide Primzahlen p, q von der Form $4z+1$ sind, es vier Faktoren r giebt, für welche $s = r$ wird, und ihr Produkt ist

$$\left.\begin{aligned} 1 \cdot \varrho \cdot \sigma \cdot \sigma' &\equiv \varrho^2 \cdot \sigma^2 \equiv -1 \\ \text{oder} \quad 1 \cdot \varrho \cdot \sigma \cdot (pq - \sigma') &\equiv -\varrho^2 \sigma^2 \equiv 1 \end{aligned}\right\} \pmod{pq},$$

während die übrigen Faktoren von P paarweise zusammengefafst werden können zu Produkten, welche $\equiv \pm 1 \pmod{pq}$ sind; im ganzen kommt also

$$P \equiv \varepsilon \pmod{pq},$$

wo ε eine Einheit bedeutet. Ist dagegen mindestens eine der Primzahlen p, q von der Form $4z+3$, so sind nur die beiden Faktoren $r=1$, $r=\varrho$ vorhanden, deren zugehöriges s gleich r ist, und man findet folglich

$$P \equiv \varrho\,\varepsilon \pmod{pq},$$

wo wieder ε eine Einheit bedeutet.

Im erstern Falle folgt $P \equiv \varepsilon \pmod{p}$, $P \equiv \varepsilon \pmod{q}$ d. h., wenn P_p, P_q die absolut kleinsten Reste von P nach den beiden Moduln p, q resp. bedeuten,

$$P_p \cdot P_q = 1. \tag{230}$$

Im zweiten Falle ist $P \equiv \varrho\varepsilon \pmod{p}$ und $P \equiv \varrho\,\varepsilon \pmod{q}$, wo $\varrho^2 \equiv 1 \pmod{pq}$ also auch $\varrho^2 \equiv 1 \pmod{p}$, $\varrho^2 \equiv 1 \pmod{q}$ ist; aber ϱ kann nicht nach beiden Moduln derselben Einheit gleich sein, denn wäre

$$\varrho \equiv 1 \pmod{p}, \quad \varrho \equiv 1 \pmod{q},$$

so wäre auch $\varrho \equiv 1 \pmod{pq}$ gegen die Bedeutung von ϱ; wäre

$$\varrho \equiv -1 \pmod{p}, \quad \varrho \equiv -1 \pmod{q},$$

so wäre auch $\varrho \equiv -1 \equiv pq-1 \pmod{pq}$, wieder gegen die Bedeutung von ϱ. Daraus schliefst man, dafs $P \equiv \pm\varepsilon \pmod{p}$, $P \equiv \mp\varepsilon \pmod{q}$, also

$$P_p \cdot P_q = -1 \tag{231}$$

sein mufs. Die beiden Fälle (230), (231) können, wie leicht zu bestätigen, in der einzigen Formel

$$P_p \cdot P_q = (-1)^{\frac{(p+1)(q+1)}{4}-1} \tag{232}$$

zusammengefafst werden.

Nachdem dies erhalten worden, schreibe man nun die Gleichung (229), wie folgt:

$$P \cdot q \cdot 2q \cdots \frac{p-1}{2}q = \frac{\Pi}{p \cdot 2p \cdots \frac{q-1}{2}p}, \tag{233}$$

wo die rechte Seite nichts anderes ist, als das Produkt

$$\Big[1 \cdot 2 \cdots (p-1)\Big] \cdot \Big[(p+1)\,(p+2) \cdots (2p-1)\Big]$$
$$\cdots\Big[\Big(\frac{q-1}{2}p+1\Big)\Big(\frac{q-1}{2}p+2\Big)\cdots\Big(\frac{q-1}{2}p+\frac{p-1}{2}\Big)\Big],$$

dessen einzelne Teilprodukte, mit Ausnahme des letzten, welches

$$\equiv 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \pmod{p}$$

ist, dem Wilsonschen Satze zufolge $\equiv -1 \pmod{p}$ sind. Deshalb ergiebt die Gleichung (233) die nachstehende Kongruenz:

$$P_p \cdot 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \cdot q^{\frac{p-1}{2}} \equiv (-1)^{\frac{q-1}{2}} \cdot 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \pmod{p}$$

oder, vereinfacht und mit Rücksicht auf das Eulersche Kriterium,

$$P_p \cdot \left(\frac{q}{p}\right) \equiv (-1)^{\frac{q-1}{2}} \pmod{p},$$

also, da P_p eine Einheit ist, die folgende Gleichheit:

$$P_p \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}}.$$

Ganz ebenso aber erschliefst man aus der Gleichung

$$(234) \qquad P \cdot p \cdot 2p \cdots \frac{q-1}{2} p = \frac{\Pi}{q \cdot 2q \cdots \frac{p-1}{2} q}$$

die Gleichheit

$$P_q \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}},$$

die, mit der vorigen verbunden und mit Benutzung der Formel (232), die fernere liefert:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p+1)(q+1)}{4} + \frac{p-1}{2} + \frac{q-1}{2} - 1}$$

d. i.

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

das Legendresche Reziprozitätsgesetz.

Man ersieht aus der Gleichung (233), aus welcher, wenn man rechts und links die Faktoren zählt, deren Reste (mod. p) gröfser sind als $\frac{p}{2}$, sogleich die der Formel (105) entsprechende Beziehung

$$\gamma + \delta + \mu\,(q,p) = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

abgelesen werden kann, ebenso wie aus der Gleichung (234) die der Formel (104) entsprechende Formel

$$\beta + \delta + \mu\,(p,q) = \frac{p-1}{2} \cdot \frac{q-1}{2},$$

noch näher, in wie engem Zusammenhange dieser Beweis mit dem fünften Gaufsschen steht. Da im letztern das Reziprozitätsgesetz

aus den eben geschriebenen Gleichungen in Verbindung mit der dritten Beziehung

$$\alpha + \delta = \beta + \gamma = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

erschlossen wird, so wird diese letzte Beziehung im Schmidtschen Beweise durch die Formel (232) vertreten, und in diesem Ersatze der einen Beziehung durch die andere besteht im Grunde das Eigentümliche des dargestellten Beweises.

25. Schmidt hat demselben noch einen dritten Beweis hinzugefügt, der gewissermafsen aus den beiden ersten herauswächst, und hat ihm sogar zwei Fassungen gegeben; doch setzt die erstere von ihnen, gerade wie Legendre's frühester Beweisversuch, das Vorhandensein von Primzahlen in gewissen arithmetischen Progressionen voraus. Wir teilen daher nur die zweite Fassung mit, die den Beweis zur Klasse der Induktionsbeweise reiht; im übrigen erinnert derselbe an den vorigen dadurch, dafs er sich des verallgemeinerten Gaufsschen Lemma für den Modulus PQ bedient, also auf die Betrachtung der Zahlenreihe $1, 2, 3, \cdots \frac{PQ-1}{2}$ begründet ist, durch einen andern, nachher zu erwähnenden Umstand aber auch an den ersten der drei Beweise.

Zunächst giebt Schmidt eine Herleitung des genannten Lemmas, die im Grunde auf die von Schering gegebene hinauskommt, und daher übergangen werden kann. Demselben zufolge ist bekanntlich

$$\left(\frac{m}{n}\right) = (-1)^{\mu(m,n)}, \tag{235}$$

wenn n eine positive ungerade, m eine positive zu n prime Zahl, und $\mu(m, n)$ die Anzahl der negativen absolut kleinsten Reste der Vielfachen

$$1 \cdot m,\ 2 \cdot m,\ 3 \cdot m, \cdots \frac{n-1}{2} m \pmod{n} \tag{236}$$

bezeichnet, und demgemäfs besagt das Reziprozitätsgesetz zwischen zwei ungeraden, relativ primen, positiven Zahlen P, Q nichts anderes als die Kongruenz:

$$\mu(P, Q) + \mu(Q, P) \equiv \frac{P-1}{2} \cdot \frac{Q-1}{2} \pmod{2}. \tag{237}$$

Setzt man ferner $n = PQ$, m also als eine sowohl zu P als zu Q relativ prime Zahl voraus, so folgt aus den Formeln

$$\left(\frac{m}{P}\right) = (-1)^{\mu(m,P)},\ \left(\frac{m}{Q}\right) = (-1)^{\mu(m,Q)}$$

$$\left(\frac{m}{PQ}\right) = (-1)^{\mu(m,PQ)}$$

und aus den Eigenschaften des Jacobischen Symbols die zweite Kongruenz:

(238) $$\mu(m, P) + \mu(m, Q) \equiv \mu(m, PQ) \pmod{2}.$$

Diese Hilfsmittel genügen zum Beweise des Reziprozitätsgesetzes, das hier wieder nur in seiner einfachen, auf zwei Primzahlen bezüglichen Form abgeleitet wird. Wir nehmen wieder an, dies Gesetz bestehe für je zwei ungerade Primzahlen, welche kleiner sind als eine gegebene Primzahl q, und weisen nach, dafs es dann auch für jede Kombination dieser Primzahl q mit einer der kleineren Primzahlen p besteht. Aus der Annahme aber folgt, wie früher hervorgehoben, dafs das Gesetz auch zwischen irgend zwei positiven ungeraden Zahlen als giltig anzusehen ist, die nur aus solchen kleineren Primzahlen zusammengesetzt sind.

Sei nun p irgend eine ungerade Primzahl $< q$; da man x so wählen kann, dafs $qx \equiv 1 \pmod{p}$, und hier, wenn x gerade also $p - x$ ungerade wäre, $q(p-x) \equiv -1 \pmod{p}$ würde, so giebt es eine positive ungerade, zu p prime Zahl $h < p$, der Art, dafs bei passend gewählter Einheit ε die Kongruenz $qh \equiv \varepsilon \pmod{p}$ oder die Gleichung

(239) $$qh = 2ip + \varepsilon$$

besteht. Falls $\varepsilon = +1$ ist, folgt dann

$$\left(\frac{qh}{p}\right) = (-1)^{\mu(q,p) + \mu(h,p)} = 1$$

oder

$$\mu(q, p) + \mu(h, p) \equiv 0 \pmod{2}.$$

Ist aber $\varepsilon = -1$, so folgt

$$\left(\frac{qh}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

und daher findet sich dann dieselbe Summe $\equiv \frac{p-1}{2} \pmod{2}$. Allgemein also ist

(240) $$\mu(q, p) + \mu(h, p) \equiv \frac{1-\varepsilon}{2} \cdot \frac{p-1}{2} \pmod{2}.$$

Da ferner $h < p < q$ ist, gilt zwischen den positiven ungeraden, relativ primen Zahlen h, p, die nur aus Primzahlen $< q$ zusammengesetzt sind, das verallgemeinerte Reziprozitätsgesetz, dem die Kongruenz

(241) $$\mu(h, p) + \mu(p, h) \equiv \frac{p-1}{2} \cdot \frac{h-1}{2} \pmod{2}$$

Ausdruck giebt; endlich ist nach (238)

(242) $$\mu(p, qh) \equiv \mu(p, q) + \mu(p, h) \pmod{2}.$$

Betrachte man nun zuerst den Fall $\varepsilon = 1$ d. h. den Fall

$$hq = 2ip + 1,\ \frac{hq-1}{2} = ip.$$

Die Reihe der Vielfachen

$$1 \cdot p,\ 2 \cdot p,\ 3 \cdot p, \cdots \frac{hq-1}{2} p = ip \cdot p,$$

für welche $\mu(p, qh)$ die Anzahl der absolut hleinsten Reste (mod. hq), welche negativ sind, angiebt, läfst sich — hier tritt die Ähnlichkeit ein, welche dieser dritte Beweis mit dem ersten hat — folgendermafsen in $\frac{p+1}{2}$ Abschnitte zerlegen:

$$p,\ 2p, \cdots ip, \quad (i+1)p \cdots 2ip;$$
$$2ip + p,\ 2ip + 2p, \cdots 2ip + ip, \quad 2ip + (i+1)p, \cdots 4ip;$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$(p-1)\, ip + p, \cdots (p-1)\, ip + ip;$$

die absolut kleinsten Reste dieser Zahlen (mod. hq) aber sind:

$$p,\ 2p, \cdots, ip,\ -(i-1)p - 1, \cdots -1;$$
$$p-1,\ 2p-1, \cdots ip-1,\ -(i-1)p-2, \cdots -2;$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$p - \frac{p-1}{2}, \cdots, ip - \frac{p-1}{2};$$

unter ihnen befinden sich $i \cdot \frac{p-1}{2}$ negative, folglich ist

$$\mu(p, qh) = i \cdot \frac{p-1}{2}.$$

Sei zweitens $\varepsilon = -1$ d. h.

$$hq = 2ip - 1, \frac{hq-1}{2} = ip - 1.$$

In diesem Falle handelt es sich um die Vielfachen

$$1p,\ 2p,\ 3p, \cdots (ip-1)p,$$

welche man wieder in Abschnitte zerlegen kann, wie folgt:

$$\begin{array}{llllll} * & p, & 2p, & \cdots (i-1)p, & ip, & \cdots (2i-1)p; \\ 2ip, & (2i+1)p, & (2i+2)p, & \cdots (3i-1)p, & 3ip, & \cdots (4i-1)p; \\ 4ip, & (4i+1)p, & (4i+2)p, & \cdots (5i-1)p, & 5ip, & \cdots (6i-1)p; \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ (p-1)ip, & \ldots & & & & \ldots (pi-1)p; \end{array}$$

die absolut kleinsten Reste dieser Zahlen (mod. hq) aber sind:

$$\begin{array}{llllll} * & p, & 2p, & \cdots (i-1)p, & -(ip-1), & \cdots -(p-1); \\ 1, & 1+p, & 1+2p, & \cdots 1+(i-1)p, & -(ip-2), & \cdots -(p-2); \\ 2, & 2+p, & 2+2p, & \cdots 2+(i-1)p, & -(ip-3), & \cdots -(p-3); \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \frac{p-1}{2}, & \frac{p-1}{2}+p, & \ldots & \frac{p-1}{2}+(i-1)p; & & \end{array}$$

auch unter diesen befinden sich $i \cdot \frac{p-1}{2}$ negative absolut kleinste Reste, und demnach ist wieder

$$\mu(p, qh) = i \cdot \frac{p-1}{2}.$$

Daher nimmt die Formel (242) nunmehr die Gestalt an:

$$(243) \qquad \mu(p, q) + \mu(p, h) \equiv i \cdot \frac{p-1}{2} \pmod{2};$$

die Kongruenzen (240), (241), (243) aber bleiben bestehen, wenn man ihre rechten Seiten mit den ungeraden Zahlen $-q$, $-q$, p resp. multipliziert, und wenn man alsdann ihre Summe bildet und die Gleichung (239) in Betracht zieht, findet sich sogleich

$$\mu(p, q) + \mu(q, p) \equiv \frac{p-1}{2} \cdot \frac{q\varepsilon - \varepsilon}{2} \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod{2};$$

da somit das Reziprozitätsgesetz auch noch für die Kombination p, q in Bestand bleibt, ist es allgemein erwiesen.

26. Wir beenden die Reihe der Beweise desselben, indem wir noch den Beweis von **Zolotareff** (*Nouv. Ann. de Math.* (2) 11, 1872, p. 354) zur Darstellung bringen, der durch die eigentümliche Transformation des Gaufsschen Lemma, die er verwendet, von besonderem Interesse ist.

Zu diesem Zwecke soll zunächst der Satz, in welchem sie zum Ausdrucke kommt, für den einfachen Fall zweier ungerader Primzahlen p, q, auf welchen sich Zolotareff beschränkt, nach seinem Vorgange hergeleitet werden. Jedoch ist der Satz später durch Lerch (*Bull. international* 3, *Prague* 1896, *sur un théorème arithmétique de Zolotarev*) verallgemeinert worden und gestattet uns, den Beweis von Zolotareff dann sogleich für das verallgemeinerte Reziprozitätsgesetz zu führen.

Sei also zunächst p eine ungerade Primzahl und die positive ganze Zahl k prim zu p, dann bilden zunächst die kleinsten positiven Reste der Vielfachen

$$(244) \qquad 1k, 2k, 3k, \cdots (p-1)k \pmod{p}$$

eine Permutation der Zahlen

$$(245) \qquad 1, 2, 3, \cdots p-1;$$

legt man dieser den Charakter $+1$ oder -1 bei, jenachdem sie aus der Reihe (245) durch eine gerade oder eine ungerade Anzahl von Transpositionen zweier Zahlen hervorgeht, so ist jener Charakter gleich $\left(\frac{k}{p}\right)$.

Um dies zu zeigen, sei g (vgl. Nr. 5) eine primitive Wurzel von p; später wird gezeigt werden, dafs dann die Reste der Potenzen

$$(246) \qquad 1,\, g,\, g^2, \cdots g^{p-2}$$

(mod. p) unter einander verschieden sind, also gleichfalls eine Permutation der Zahlen (245) darstellen, sodaſs es eine gewisse Potenz g^c jener Reihe giebt, welche mit k kongruent wird: $g^c \equiv k$ (mod. p). Daher entsteht die Reihe der Reste der Produkte

$$k,\, kg,\, kg^2, \cdots kg^{p-2}$$

oder der Potenzen

$$(247) \qquad g^c,\, g^{c+1},\, g^{c+2}, \cdots g^{c+p-2}$$

aus der Reihe der Reste von (246) genau durch die gleichen Permutationen, wie die Permutation (244) aus der Reihe (245); offenbar entsteht aber (247) aus (246) durch die c-fach wiederholte cyklische Permutation $p-1^{\text{ter}}$ Ordnung:

$$\begin{pmatrix} 1, & g, & g^2, & \cdots g^{p-2} \\ g, & g^2, & g^3, & \cdots g^{p-1} \end{pmatrix},$$

welche durch $p-2$ Transpositionen hervorgebracht wird, ist also $c(p-2)$ Transpositionen äquivalent, deren Anzahl zugleich mit c gerade oder ungerade ist; je nach diesen Fällen ist aber $k \equiv g^c$, da g quadratischer Nichtrest ist von p (vgl. Nr. 5), quadr. Rest oder Nichtrest, d. h. ist $\left(\frac{k}{p}\right) = +1$ oder -1, w. z. b. w. —

Man kann aber, wie bemerkt, diesen Satz verallgemeinern, und die Art, wie es von Lerch gethan worden ist, zeigt zugleich, daſs er nichts anderes ist, als eine neue Deutung des Gauſsschen Lemma. Verstehen wir unter einer Verstellung (dérangement) zweier Zahlen der Reihe (245) den Umstand, daſs in einer Permutation dieser Zahlenreihe die kleinere jener beiden Zahlen später steht, als die gröſsere, so ist die Anzahl der Verstellungen, die eine Permutation aufweist, wie leicht zu sehen, immer gleichzeitig mit der Anzahl von Transpositionen, durch welche die Permutation entsteht, gerade oder ungerade. Dies vorausbemerkt, sei jetzt p eine beliebige positive ganze Zahl und k prim gegen sie, also ungerade, falls p gerade ist; ferner sei

$$\varrho(x) = x - [x].$$

Indem man an die Stelle der Reihen (244), (245) die mit p dividierten Zahlen betrachtet, wird die Restreihe von (244) übergehen in die Reihe

$$\varrho\left(\frac{k}{p}\right),\quad \varrho\left(\frac{2k}{p}\right), \cdots \varrho\left(\frac{(p-1)k}{p}\right),$$

welche eine Permutation der Reihe

$$\frac{1}{p},\, \frac{2}{p}, \cdots \frac{p-1}{p}$$

sein muſs, und die Anzahl der Verstellungen in dieser Permutation wird gerade oder ungerade sein, jenachdem das Produkt

$$\prod\left[\varrho\left(\frac{hk}{p}\right)-\varrho\left(\frac{h'k}{p}\right)\right]$$
$$(\text{für } h > h' = 1, 2, 3, \cdots p-2)$$

positiv oder negativ ausfällt. Nun ist für $x > x'$, wie unmittelbar zu übersehen ist,

$$[x]-[x']-[x-x'] = 0 \text{ oder } 1,$$

jenachdem

$$\varrho(x)-\varrho(x') > 0 \text{ oder } < 0$$

ist. Demnach wird das Vorzeichen des Produktes mit dem der Potenz

$$(-1)^{\sum\limits_{h=2}^{p-1}\sum\limits_{h'=1}^{h-1}\left(\left[\frac{hk}{p}\right]-\left[\frac{h'k}{p}\right]-\left[\frac{(h-h')k}{p}\right]\right)}.$$

identisch sein, diese Potenz also den Charakter der fraglichen Permutation ausmachen. Es ist aber

$$\sum_{h,h'}\left[\frac{(h-h')k}{p}\right]=\sum_{h=2}^{p-1}\sum_{h''=1}^{h-1}\left[\frac{h''k}{p}\right],$$

wo man den Summationsbuchstaben h'' auch wieder h' nennen kann, und somit darf der Exponent jener Potenz einfach durch die Summe

$$\sum_{h=2}^{p-1}\sum_{h'=1}^{h-1}\left[\frac{hk}{p}\right]=\sum_{h=2}^{p-1}(h-1)\left[\frac{hk}{p}\right]$$

oder, da man die den ungeraden h entsprechenden geradzahligen Teile unterdrücken, die den geraden h entsprechenden Teile durch $\left[\frac{hk}{p}\right]$ ersetzen darf, noch einfacher durch

$$\sum_{h=1}^{\left[\frac{p-1}{2}\right]}\left[\frac{2hk}{p}\right] \tag{248}$$

ersetzt werden, ohne den Wert der Potenz von -1 zu verändern. Da $(-1)^{[2x]} = \text{sgn.}\, R(x)$, so ist mithin der Charakter der fraglichen Permutation nichts anderes als

$$\prod_{h=1}^{\left[\frac{p-1}{2}\right]}\text{sgn.}\, R\left(\frac{hk}{p}\right). \tag{249}$$

Für den Fall also, wo p ungerade ist, gilt der verallgemeinerte **Zolotareffsche** Satz, nach welchem der Charakter der Permutation der Reste von (244) (mod. p) durch das Symbol $\left(\frac{k}{p}\right)$ auch dann ausgedrückt wird, wenn p keine Primzahl ist.

Um aber auch den Fall eines geraden p nicht zu übergehen, beweisen wir, dafs in diesem Falle die Summe (248) gleich $\frac{k-1}{2}\cdot\left(\frac{p}{2}-1\right)$ ist. Sei nämlich zuerst $\frac{p}{2}-1$ gerade, dann kann man die Glieder der Summe paarweise zusammenfassen und für jedes Paar ist

$$\left[\frac{2hk}{p}\right]+\left[\frac{\left(\frac{p}{2}-h\right)2k}{p}\right]=k-1,$$

die Summe also gleich $\frac{1}{2}\left(\frac{p}{2}-1\right)\cdot(k-1)$. Ist aber $\frac{p}{2}-1$ ungerade d. h. $\frac{p}{4}$ eine ganze Zahl, so wird bei solcher paarweisen Zusammenfassung der Glieder, während sonst alles bleibt wie zuvor, noch ein mittleres isoliertes Glied vorhanden sein:

$$\left[\frac{p}{4}\cdot\frac{2k}{p}\right]=\left[\frac{k}{2}\right]=\frac{k-1}{2},$$

folglich wird die Summe gleich

$$\frac{k-1}{2}+\frac{1}{2}\left(\frac{p}{2}-2\right)\cdot(k-1)=\frac{k-1}{2}\cdot\left(\frac{p}{2}-1\right).$$

Im Falle eines geraden p ist also der Charakter der fraglichen Permutation

$$(-1)^{\frac{k-1}{2}\cdot\left(\frac{p}{2}-1\right)}.$$

(S. hierzu Schering, *Abh. der Gött. Ges.* 24, 1879, „Bestimmung des quadr. Restcharakters“ p. 35.)

Seien nunmehr wieder P, Q zwei positive ungerade Zahlen ohne gemeinsamen Teiler. Die Zahlen

$$(250)\qquad 0,\ 1,\ 2,\ 3,\cdots PQ-1$$

werden mit den Resten der Zahlen

$$Px+Qy$$
$$(\text{für } x=0,\ 1,\ 2,\cdots Q-1;\quad y=0,\ 1,\ 2,\cdots P-1)$$

(mod. PQ) in gewisser Reihenfolge übereinstimmen. Die letztbezeichneten Zahlen nun stellen wir dar in dem Schema:

$$(251)\left\{\begin{array}{lllll} 0, & Q, & 2Q, & \cdots & (P-1)Q \\ P, & P+Q, & P+2Q, & \cdots & P+(P-1)Q \\ 2P, & 2P+Q, & 2P+2Q, & \cdots & 2P+(P-1)Q \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ (Q-1)P, & (Q-1)P+Q, & & \cdots & (Q-1)P+(P-1)Q, \end{array}\right.$$

dessen Zahlen wir in der Reihenfolge gelesen denken, wie sich die Horizontalreihen von links nach rechts hin aneinanderschliefsen; die

Reste der so geordneten Zahlen bilden also eine gewisse Permutation der Reihe (250).

Vertauscht man in (251) die Kolonnen in der Weise, daſs die Reste von

$$0,\ Q,\ 2Q, \cdots (P-1)Q \pmod{P}$$

die Reihe $0, 1, 2, \cdots P-1$ bilden, so nimmt das Schema die neue Gestalt an:

$$(252)\left\{\begin{array}{lllll} 0, & Pk_1+1, & Pk_2+2, & \cdots & Pk_{P-1}+P-1 \\ P, & P(1+k_1)+1 & P(1+k_2)+2, & \cdots & P(1+k_{P-1})+P-1 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ (Q-1)P, & P(Q-1+k_1)+1, & & \cdots & P(Q-1+k_{P-1})+P-1. \end{array}\right.$$

Nach dem voraufgeschickten Hilfssatze bedarf es zu solcher Vertauschung einer geraden oder ungeraden Anzahl von Transpositionen zweier Kolonnen, jenachdem $\left(\frac{Q}{P}\right) = +1$ oder -1 ist; die erforderliche Anzahl von Transpositionen zweier Elemente ist Q Mal so groſs, da jede Kolonne aus Q Elementen besteht, ist mithin ebenfalls gerade oder ungerade, jenachdem $\left(\frac{Q}{P}\right)$ den ersten oder den zweiten Wert hat, sie ist mit anderen Worten

$$\equiv \frac{1}{2}\left(\left(\frac{Q}{P}\right)-1\right) \pmod{2}.$$

Nun entstehen die Glieder einer der $P-1$ letzten Kolonnen des letzten Schema, nämlich die Glieder

$$(253)\qquad Pk_i+i,\ \ P(1+k_i)+i, \cdots P(Q-1+k_i)+i,$$

wenn man nur ihre Reste (mod. PQ) betrachtet, aus den Zahlen

$$(254)\qquad i,\ \ P+i, \cdots P(Q-1)+i$$

durch eine k_i Mal wiederholte cyklische Vertauschung, deren jede $Q-1$ Transpositionen äquivalent ist; es bedarf also, um den Übergang von (254) zu (253) zu machen, und natürlich auch für den umgekehrten Übergang einer geraden Anzahl von Transpositionen. Da dies für jeden der Werte $i = 1, 2, 3, \cdots P-1$ gilt, so geht das Restschema (252) durch eine gerade Anzahl von Transpositionen zweier Zahlen in das nachstehende über:

$$\begin{array}{c} 0,\ 1,\ 2, \cdots P-1, \\ P,\ P+1,\ P+2, \cdots 2P-1, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ (Q-1)P,\ \ (Q-1)P+1, \cdots QP-1, \end{array}$$

welches, da es zu lesen ist wie die Horizontalreihen von links nach rechts hin sich an einander schlieſsen, mit der Reihe (250) überein-

stimmt. Man findet also, dafs die Anzahl der Transpositionen, durch welche man von (251) zu (250) übergeht,

$$\equiv \frac{1}{2}\left(\left(\frac{Q}{P}\right)-1\right) \pmod{2}$$

ist.

Aber man kann diesen Übergang auch auf folgende andere Art bewerkstelligen. Indem man zunächst mit den Horizontalreihen ebenso operiert, wie vorher mit den Kolonnen, kann man durch eine Anzahl von Transpositionen, welche

$$\equiv \frac{1}{2}\left(\left(\frac{P}{Q}\right)-1\right) \pmod{2}$$

ist, von (251) zunächst zu folgendem Schema gelangen:

$$\begin{array}{lllll}
0, & Q, & 2Q, & \cdots & (P-1)Q, \\
1, & Q+1, & 2Q+1, & \cdots & (P-1)Q+1, \\
2, & Q+2, & 2Q+2, & \cdots & (P-1)Q+2, \\
\cdot & \cdot & \cdot & \cdot & \cdot \\
Q-1, & 2Q-1, & 3Q-1, & \cdots & PQ-1,
\end{array}$$

das wieder nach den aneinanderschliefsenden Horizontalreihen zu lesen ist. Hierin aber setzt man durch $P-1$ Transpositionen die Zahl 1 an die erste auf 0 folgende Stelle, durch $2(P-1)$ Transpositionen dann die Zahl 2 an die zweite, u. s. w., durch $(Q-1)(P-1)$ Transpositionen die Zahl $Q-1$ an die $(Q-1)^{\text{te}}$ Stelle nach der Zahl 0, führt also durch

$$\frac{Q(Q-1)}{1\cdot 2}\cdot(P-1)$$

Transpositionen die Anordnung

$$0,\ 1,\ 2,\ \cdots (Q-1),\ Q,\ 2Q,\ \cdots (P-1)Q,\ Q+1,\ 2Q+1,\ \cdots \\ (P-1)Q+1,\ Q+2,\ \cdots$$

herbei; desgleichen nunmehr durch

$$\frac{Q(Q-1)}{1\cdot 2}\cdot(P-2)$$

Transpositionen die neue Anordnung

$$0,\ 1,\ 2,\ (Q-1),\ Q,\ Q+1,\ Q+2,\ \cdots 2Q-1,\ 2Q,\ \cdots \\ (P-1)Q,\ 2Q+1,\ \cdots (P-1)Q+1,\ 2Q+2,\ \cdots,$$

u. s. w., und erhält so endlich die Reihe (250) durch im Ganzen

$$\frac{Q(Q-1)}{1\cdot 2}\cdot\frac{P(P-1)}{1\cdot 2}$$

Transpositionen. Demnach geht bei dieser zweiten Methode das Schema (251) in die Reihe (250) über durch eine Anzahl von Transpositionen, welche

$$\equiv \frac{1}{2}\left(\left(\frac{P}{Q}\right)-1\right)+\frac{P(P-1)}{2}\cdot\frac{Q(Q-1)}{2} \pmod{2}$$

ist. Da diese Anzahl mit derjenigen, welche bei der ersten Methode als erforderlich gefunden worden, zugleich gerade resp. ungerade sein mufs, so ergiebt sich die Kongruenz

$$\left.\begin{aligned}\frac{1}{2}\left(\left(\frac{Q}{P}\right)-1\right) &\equiv \frac{1}{2}\left(\left(\frac{P}{Q}\right)-1\right)+\frac{P(P-1)}{2}\cdot\frac{Q(Q-1)}{2}\\ &\equiv \frac{1}{2}\left(\left(\frac{P}{Q}\right)-1\right)+\frac{P-1}{2}\cdot\frac{Q-1}{2}\end{aligned}\right\} \pmod{2}.$$

Ist also wenigstens eine der Zahlen P, Q von der Form $4z+1$, so ist

$$\frac{1}{2}\left(\left(\frac{Q}{P}\right)-1\right) \equiv \frac{1}{2}\left(\left(\frac{P}{Q}\right)-1\right) \pmod{2},$$

was dann und nur dann der Fall, wenn

$$\left(\frac{Q}{P}\right)=\left(\frac{P}{Q}\right);$$

im entgegengesetzten Falle ist

$$\frac{1}{2}\left(\left(\frac{Q}{P}\right)-1\right) \equiv \frac{1}{2}\left(\left(\frac{P}{Q}\right)-1\right)+1 \pmod{2},$$

was dann und nur dann eintritt, wenn

$$\left(\frac{Q}{P}\right)=-\left(\frac{P}{Q}\right)$$

ist; das Reziprozitätsgesetz ist also bewiesen. —

27. Nach dieser ausführlichen Betrachtung des Reziprozitätsgesetzes wenden wir uns nunmehr zu der Aufgabe, zu entscheiden, ob eine gegebene Zahl m von einer gegen sie primen (positiven) ungeraden Primzahl p quadratischer Rest oder Nichtrest ist, allgemeiner zu der Aufgabe, den quadratischen Charakter von m bezüglich einer gegen sie primen ungeraden (positiven) Zahl n zu bestimmen, wieder zurück. Durch die beiden Ergänzungssätze ist diese Aufgabe bezüglich der Zahlen $m=1$ und $m=2$ mittels der Formeln (53) und (55) bereits für jede der Zahlen n gelöst:

$$\left(\frac{-1}{n}\right) \text{ ist } \begin{array}{ll} +1 & \text{für alle Zahlen } n=4z+1,\\ -1 & \text{„ „ „ } n=4z+3,\end{array}$$

$$\left(\frac{2}{n}\right) \text{ ist } \begin{array}{ll} +1 & \text{für alle Zahlen } n=8z+1,\ n=8z+7,\\ -1 & \text{„ „ „ } n=8z+3,\ n=8z+5.\end{array}$$

Hieraus schliefst man sogleich noch weiter:

$\left(\frac{-2}{n}\right)$ ist $+1$ für alle Zahlen $n = 8z+1$, $n = 8z+3$,
-1 „ „ „ $n = 8z+5$, $n = 8z+7$.

Man bemerke, dafs hiernach sämtliche Zahlen n, für welche -1 einen bestimmten quadratischen Charakter hat, die Zahlen sind, welche in **einer**, diejenigen Zahlen n, für welche ± 2 einen bestimmten quadratischen Charakter hat, die Zahlen sind, welche in **zwei** gewissen arithmetischen Progressionen enthalten sind.

Ungelöst blieb einstweilen die Bestimmung des quadratischen Charakters $\left(\frac{m}{n}\right)$ für einen von ± 1, ± 2 verschiedenen Wert von m. Wir zeigen zuerst, dafs auch hier alle Zahlen n, für welche das Symbol $\left(\frac{m}{n}\right)$ einen bestimmten der Werte ± 1 hat, mit den in einer Anzahl gewisser arithmetischer Progressionen enthaltenen Zahlen identisch sind. Hierzu bemerken wir zunächst, dafs die Zahl m, welche positiv oder negativ, gerade oder ungerade sein kann, sich immer in die Gestalt

$$m = \pm 2^c r s^2$$

setzen läfst, wo $c = 0$ oder 1, und r eine nur aus verschiedenen ungeraden Primfaktoren zusammengesetzte Zahl oder die Einheit ist. Da

$$\left(\frac{m}{n}\right) = \left(\frac{\pm 2^c r s^2}{n}\right) = \left(\frac{\pm 2^c r}{n}\right)$$

ist, dürfen wir uns auf den einfachsten Fall

$$m = \pm 2^c r \tag{255}$$

beschränken. Hierbei darf r von 1 verschieden gedacht werden, da man sonst auf die bereits erledigten Werte ± 1, ± 2 von m zurückkäme. Dann findet man aber mittels des verallgemeinerten Reziprozitätsgesetzes und des zweiten Ergänzungssatzes

$$\left(\frac{m}{n}\right) = (-1)^{c \cdot \frac{n^2-1}{8}} \cdot (-1)^{\frac{n-1}{2} \cdot \frac{\pm r - 1}{2}} \cdot \left(\frac{n}{r}\right).$$

Setzt man also

$$(-1)^{\frac{\pm r-1}{2}} = \delta, \quad (-1)^c = \varepsilon,$$

d. h., setzt man $\delta = +1$ oder -1, jenachdem $\pm r \equiv 1$ oder $\equiv 3$ (mod. 4) ist, und $\varepsilon = +1$ oder -1, jenachdem $c = 0$ oder 1 ist, so besteht die Formel

$$\left(\frac{m}{n}\right) = \delta^{\frac{n-1}{2}} \cdot \varepsilon^{\frac{n^2-1}{8}} \cdot \left(\frac{n}{r}\right); \tag{256}$$

ihr zufolge aber wird das Symbol $\left(\frac{m}{n}\right)$ für je zwei (mod. $8r$), wenn $\varepsilon = +1$ ist, schon für je zwei (mod. $4r$), und wenn auch $\delta = +1$ ist, sogar schon für je zwei (mod. $2r$) kongruente Werte von n denselben Wert haben; es wird also nur darauf ankommen, diejenigen n zu betrachten, welche ein reduziertes Restsystem nach diesen Moduln resp. bilden.

Nun wollen wir in dem reduzierten Restsysteme (mod. $2r$) diejenigen Zahlen n, für welche $\left(\frac{n}{r}\right) = 1$ ist, durch den Buchstaben a, diejenigen, für welche $\left(\frac{n}{r}\right) = -1$ ist, durch den Buchstaben b bezeichnen. Die Anzahl der Zahlen a ist gleich der Anzahl der Zahlen b. In der That giebt es zunächst eine Zahl der zweiten Kategorie. Denn, sei p eine in r aufgehende Primzahl, also $r = pr'$, r' also nicht teilbar durch p, und sei β irgend ein Nichtrest von p; bestimmt man dann b_0 durch die mit einander verträglichen Kongruenzen

$$b_0 \equiv \beta \pmod{p}, \quad b_0 \equiv 1 \pmod{r'},$$

so wird, wie es behauptet wurde, $\left(\frac{b_0}{r}\right) = \left(\frac{b_0}{pr'}\right) = \left(\frac{\beta}{p}\right)\left(\frac{1}{r'}\right) = -1$. Multipliziert man alsdann die Gesamtheit der Zahlen a, b d. i. das reduzierte Restsystem n (mod. $2r$) mit dieser Zahl b_0, welche prim gegen r ist, aber auch ungerade gedacht werden kann, da sie andernfalls durch $b_0 + r$ ersetzt werden darf, so erhält man wieder ein reduziertes Restsystem (mod. $2r$), und folglich ist die über ein solches erstreckte Summe

$$\sum_n \left(\frac{n}{r}\right) = \sum_n \left(\frac{b_0 n}{r}\right) = \left(\frac{b_0}{r}\right) \cdot \sum_n \left(\frac{n}{r}\right) = -\sum_n \left(\frac{n}{r}\right)$$

also

$$\sum_n \left(\frac{n}{r}\right) = \sum_a \left(\frac{a}{r}\right) + \sum_b \left(\frac{b}{r}\right) = 0$$

oder die Anzahl der a gleich derjenigen der b.

Wenn nun erstens $\delta = 1$, $\varepsilon = 1$ also $m \equiv 1 \pmod{4}$ ist, wird nach der Formel (256)

$$\left(\frac{m}{n}\right) = 1, \qquad \text{wenn} \quad n \equiv a \pmod{2r},$$

$$\left(\frac{m}{n}\right) = -1, \qquad \text{wenn} \quad n \equiv b \pmod{2r};$$

die ungeraden Zahlen n, für welche $\left(\frac{m}{n}\right)$ einen bestimmten der Werte ± 1 hat, sind also identisch mit den Zahlen, welche in gewissen $\frac{1}{2}\varphi(2r) = \frac{1}{2}\varphi(r) = \frac{1}{2}\varphi(m)$ arithmetischen Progressionen mit der Differenz $2r$ oder $2m$ enthalten sind.

Wenn zweitens $\delta = -1$, $\varepsilon = 1$ also $m \equiv 3 \pmod{4}$ ist, so wird

$$\left(\frac{m}{n}\right) = 1, \quad \text{wenn entweder} \quad n \equiv 1 \pmod{4}, \quad n \equiv a \pmod{r}$$
$$\text{oder} \quad n \equiv 3 \pmod{4}, \quad n \equiv b \pmod{r},$$
$$\left(\frac{m}{n}\right) = -1, \quad \text{wenn entweder} \quad n \equiv 3 \pmod{4}, \quad n \equiv a \pmod{r}$$
$$\text{oder} \quad n \equiv 1 \pmod{4}, \quad n \equiv b \pmod{r};$$

die ungeraden n, für welche $\left(\frac{m}{n}\right)$ einen bestimmten der Werte ± 1 hat, sind also die in gewissen $\frac{1}{2}\varphi(4r) = \frac{1}{2}\varphi(4m)$ arithmetischen Progressionen mit der Differenz $4r$ oder $4m$ enthaltenen Zahlen, auf welche n durch diese Kongruenzbedingungen beschränkt wird.

Ist drittens $\delta = 1$, $\varepsilon = -1$ also $m \equiv 2 \pmod{8}$, so wird

$$\left(\frac{m}{n}\right) = 1, \quad \text{wenn entweder} \quad n \equiv 1{,}7 \pmod{8}, \quad n \equiv a \pmod{r}$$
$$\text{oder} \quad n \equiv 3{,}5 \pmod{8}, \quad n \equiv b \pmod{r},$$
$$\left(\frac{m}{n}\right) = -1, \quad \text{wenn entweder} \quad n \equiv 3{,}5 \pmod{8}, \quad n \equiv a \pmod{r}$$
$$\text{oder} \quad n \equiv 1{,}7 \pmod{8}, \quad n \equiv b \pmod{r}.$$

Ist endlich viertens $\delta = -1$, $\varepsilon = -1$ also $m \equiv 6 \pmod{8}$, so wird

$$\left(\frac{m}{n}\right) = 1, \quad \text{wenn entweder} \quad n \equiv 1{,}3 \pmod{8}, \quad n \equiv a \pmod{r}$$
$$\text{oder} \quad n \equiv 5{,}7 \pmod{8}, \quad n \equiv b \pmod{r},$$
$$\left(\frac{m}{n}\right) = -1, \quad \text{wenn entweder} \quad n \equiv 5{,}7 \pmod{8}, \quad n \equiv a \pmod{r}$$
$$\text{oder} \quad n \equiv 1{,}3 \pmod{8}, \quad n \equiv b \pmod{r}.$$

In beiden Fällen sind die ungeraden Zahlen n, für welche $\left(\frac{m}{n}\right)$ einen bestimmten Wert hat, identisch mit den Zahlen, welche in gewissen $\frac{1}{2}\varphi(8r) = \frac{1}{2}\varphi(4m)$ arithmetischen Progressionen mit der Differenz $8r$ oder $4m$ enthalten sind.

Beschränkt man sich ausschliefslich auf Primzahlen n, so sind die in den bezeichneten arithmetischen Progressionen enthaltenen Primzahlen diejenigen, von welchen die Zahl m quadratischer Rest resp. Nichtrest ist. Die ersteren pflegt man nach dem Vorgange älterer Forscher, wie Euler und Legendre, „die Teiler der Form $x^2 - my^2$“ zu nennen. So sind z. B. im erstbetrachteten Falle $\delta = 1$, $\varepsilon = 1$ alle Primzahlen, welche in einer der $\frac{1}{2}\varphi(m)$ arithmetischen Progressionen oder Linearformen $2mz + a$ enthalten sind, die

Teiler der Form $x^2 - my^2$, während keine in einer der anderen $\frac{1}{2}\varphi(m)$ Linearformen $2mz + b$ enthaltenen Primzahlen ein Teiler derselben sein kann.

28. Man kann jedoch die Formel (256) oder das Reziprozitätsgesetz mit seinen beiden Ergänzungssätzen auch verwenden, um direkt den Wert des Symbols $\left(\frac{m}{n}\right)$ zu finden. Da $\left(\frac{m'}{n}\right) = \left(\frac{m}{n}\right)$ ist, sobald $m' \equiv m \pmod{n}$, so darf man von vornherein $m < n$ voraussetzen; dann ist auch $r < n$. Man setze nun

$$n = qr + m_1, \quad m_1 < r,$$

so wird $\left(\frac{n}{r}\right) = \left(\frac{m_1}{r}\right)$, ein Symbol, dessen Wert, wenn wieder

$$m_1 = \pm 2^{c_1} \cdot r_1 s_1^2$$

gesetzt wird, nach (256) auf das andere $\left(\frac{r}{r_1}\right)$ zurückkommt, wo $r_1 < r$ ist. Setzt man demnach weiter

$$r = q_1 r_1 + m_2, \quad m_2 < r_1, \quad m_2 = \pm 2^{c_2} \cdot r_2 s_2^2,$$

so kommt man auf die Bestimmung von $\left(\frac{r_1}{r_2}\right)$ zurück, u. s. w., bei welchem Fortgange endlich der Fall eintreten mufs, dafs eine der Zahlen $r, r_1, r_2, \ldots$ der Einheit gleich, das entsprechende letzte Symbol also unmittelbar bekannt ist.

Man sieht, wie hierbei durch die vorstehenden Gleichungen der Euclidische Algorithmus zu Hilfe genommen wird, und in der That ist er in verschiedener Weise ausgebeutet worden, um Regeln oder Algorithmen aufzustellen, nach denen der Wert des Symbols $\left(\frac{m}{n}\right)$ sich ergiebt. Schon Gaufs (*Comm. Gott. rec.* 4, 1818 oder *Werke* II, p. 59) gab einen solchen Algorithmus an. Dieser gründet sich auf die bereits bei seinem dritten Beweise angeführte Formel (115), in welcher wir, wenn M, N zwei positive relativ prime Zahlen sind, deren erstere ungerade sei, $x = \frac{M}{N}$, $n = \left[\frac{N}{2}\right]$ setzen wollen; aus dieser Annahme folgt, wenn N gerade ist, oder auch wenn N ungerade und zugleich $M < N$ ist, $m = \left[\frac{M}{2}\right]$ also

$$\sum_{h=1}^{\left[\frac{N}{2}\right]} \left[\frac{hM}{N}\right] + \sum_{k=1}^{\left[\frac{M}{2}\right]} \left[\frac{kN}{M}\right] = \left[\frac{M}{2}\right] \cdot \left[\frac{N}{2}\right], \tag{257}$$

eine Beziehung, welche wegen der in Bezug auf M, N darin vorhandenen Symmetrie bei ungeraden M, N auch bestehen bleibt, wenn $M > N$ ist und welche, wenn wir uns der Bezeichnung von Busche

bedienen, ferner $\left[\frac{M}{2}\right] = M'$, $\left[\frac{N}{2}\right] = N'$ setzen, kürzer folgendermaſsen:

$$\psi(M, N) + \psi(N, M) = M' \cdot N' \tag{258}$$

geschrieben werden kann. Nun entwickle man für die beiden Zahlen M, N den gewöhnlichen Euclidischen Algorithmus:

$$\begin{aligned} M &= Nq + N_1, \\ N &= N_1 q_1 + N_2, \\ N_1 &= N_2 q_2 + N_3, \\ &\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ N_{k-1} &= N_k q_k + 1, \\ N_k &= 1 \cdot q_{k+1}, \end{aligned} \tag{259}$$

dessen vorletzte Gleichung den Rest 1 darbietet, da M, N als relativ prim vorausgesetzt sind; je zwei aufeinanderfolgende Reste N, N_1; N_1, N_2; ... sind mithin auch relativ prim. Demnach ist

$$\psi(N_1, N) + \psi(N, N_1) = N_1' \cdot N',$$

und da $\left[\frac{hM}{N}\right] = hq + \left[\frac{hN_1}{N}\right]$ ist,

$$\psi(M, N) = q \cdot \frac{N'^2 + N'}{2} + \psi(N_1, N)$$

folglich

$$\psi(M, N) = q \cdot \frac{N'^2 + N'}{2} + N' \cdot N_1' - \psi(N, N_1).$$

Auf dieselbe Weise ergiebt sich

$$\begin{aligned} -\psi(N, N_1) &= -q_1 \cdot \frac{N_1'^2 + N_1'}{2} - N_1' \cdot N_2' + \psi(N_1, N_2), \\ +\psi(N_1, N_2) &= \quad q_2 \cdot \frac{N_2'^2 + N_2'}{2} + N_2' \cdot N_3' - \psi(N_2, N_3), \\ &\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ \pm\psi(N_{k-1}, N_k) &= \pm q_k \cdot \frac{N_k'^2 + N_k'}{2} \pm N_k' \cdot \left[\frac{1}{2}\right] \mp \psi(N_k, 1), \end{aligned}$$

wo in der Schluſsgleichung das letzte wie das vorletzte Glied verschwindet. Somit geht schlieſslich die Formel hervor:

$$\begin{aligned} \psi(M, N) = q \cdot \frac{N'^2 + N'}{2} - q_1 \cdot \frac{N_1'^2 + N_1'}{2} + q_2 \cdot \frac{N_2'^2 + N_2'}{2} - \cdots \\ + N' N_1' - N_1' N_2' + N_2' N_3' - \cdots. \end{aligned} \tag{260}$$

In dem besonderen Falle zweier ungerader Zahlen M, N fand sich aber nach (114)

$$\mu(M, N) \equiv \psi(M, N) \pmod{2},$$

und somit gewährt die aus dem Euclidischen Algorithmus (259) entsprungene Formel (260) in diesem Falle sogleich die Bestimmung des Restes von $\mu(M, N)$ (mod. 2) und damit nach der Formel

$$\left(\frac{M}{N}\right) = (-1)^{\mu(M, N)}$$

die Bestimmung des Symbols $\left(\frac{M}{N}\right)$.

Zeller hat (*Gött. Nachr.* 1879, p. 197) diese Gaufssche Methode vereinfacht und folgende Regel zur Bestimmung der charakteristischen Zahl $\mu(M, N)$ aufgestellt:

Man entwickle $\frac{M}{N}$ durch den Euclidischen Algorithmus (259) in einen gewöhnlichen Kettenbruch und teile seine Quotienten $q, q_1, q_2, \ldots q_k, q_{k+1}$ in ungerad- und in geradstellige. Sind alle successiven Reste $N, N_1, N_2, \ldots$ ungerade, so bilde man die um 1 vermehrte Summe der ungeradstelligen und die Summe der geradstelligen Quotienten, oder umgekehrt die Summe der ungeradstelligen und die um 1 vermehrte Summe der geradstelligen Quotienten, jenachdem die Anzahl der Kettenbruchglieder oder k in den Gleichungen (259) gerade oder ungerade ist, und nenne diese Summen ϱ', ϱ''. Sind dagegen gerade Reste vorhanden, so bedarf es gewisser Korrekturen, nämlich: ist ein Rest N_h gerade und ist der Quotient q_h es ebenfalls, so ersetze man bei der eben angegebenen Bestimmung q_h durch Null; ist aber q_h ungerade, so zähle man bei jener Bestimmung q_h nicht mit, nehme dafür aber alle folgenden Quotienten mit entgegengesetzten Vorzeichen. Für die nach diesen Vorschriften gebildeten ϱ', ϱ'' ist dann:

$$\mu(M, N) = \frac{M - \varrho'}{4}, \quad \mu(N, M) = \frac{N - \varrho''}{4}. \tag{261}$$

Da aus (259)

$$M = Nq + N_2 q_2 + N_4 q_4 + \cdots + \frac{1 \pm 1}{2},$$
$$N = N_1 q_1 + N_3 q_3 + \cdots + \frac{1 \mp 1}{2}$$

hervorgeht, wo das obere oder untere Vorzeichen zu wählen ist, jenachdem k gerade oder ungerade ist, und da entsprechend

$$\varrho' = q + q_2 + q_4 + \cdots + \frac{1 \pm 1}{2},$$
$$\varrho'' = q_1 + q_3 + \cdots + \frac{1 \mp 1}{2}$$

gesetzt werden mufs, so darf man die Formeln (261) auch durch die folgenden ersetzen:

$$\mu(M, N) = q \cdot \frac{N-1}{4} + q_2 \cdot \frac{N_2-1}{4} + \cdots$$

$$\mu(N, M) = q_1 \cdot \frac{N_1-1}{4} + q_3 \cdot \frac{N_3-1}{4} + \cdots$$

vorausgesetzt, dafs die sämtlichen Zahlen $N, N_1, N_2, \cdots$ ungerade sind.

Für die Herleitung dieser Regeln giebt Zeller nur Andeutungen, die sich auf den letztbezeichneten besonderen Fall beziehen. Schering hat in seiner umfangreichen Arbeit (*Abh. d. Gött. Ges.* 24, 1879, *Bestimmung des quadr. Restcharakters*) das Zellersche Verfahren beträchtlich verallgemeinert, indem er der Untersuchung statt des gewöhnlichen Euclidischen Algorithmus einen beliebig gebildeten zu Grunde legt, und ist auf solche Weise auch zu einer Begründung der Zellerschen Regel gelangt; doch sind seine Betrachtungen zu komplizierter Art, als dafs hier eine Mitteilung derselben versucht werden könnte. Im übrigen weisen wir für die thatsächliche Berechnung der charakteristischen Zahl $\mu(M, N)$ auf Busche's in Nr. 18 dargestellte Untersuchungen zurück, nach denen, wenn man die Funktionen $F(M, N)$, $f(M, N)$ in der dort angegebenen Weise bestimmt hat, wegen (183) sich

$$\mu(M, N) \equiv \frac{1}{2}\Big(F(M, N) + f(M, N)\Big) \pmod{2}$$

ergiebt.

29. Für die Bestimmung von $\left(\frac{M}{N}\right)$ bedarf es nur der Kenntnis einer mit $\mu(M, N)$ gleichartigen, gleichzeitig mit ihr geraden bezw. ungeraden Zahl. Hierauf basieren andere Regeln, welche von Eisenstein, Lebesgue, Kronecker u. a. gegeben worden sind.

In der Formel

$$M = qN + N_1 \tag{262}$$

kann der Quotient q nach Belieben gerade oder ungerade gewählt werden, wenn man für den Rest $N_1 < N$ sowohl positive als negative Werte zuläfst, denn die Formel läfst sich auch so schreiben:

$$M = (q+1)N - (N - N_1). \tag{263}$$

Wählt man mit Eisenstein nur gerade Quotienten oder, was dasselbe sagt, wenn M, N als ungerade vorausgesetzt werden, nur ungerade (sei es positive, sei es negative) Reste, so nimmt der Euclidische Algorithmus diese Form an:

$$\begin{aligned} M &= 2qN + \varepsilon_1 N_1 \\ N &= 2q_1 N_1 + \varepsilon_2 N_2 \\ N_1 &= 2q_2 N_2 + \varepsilon_3 N_3 \\ &\cdots\cdots\cdots\cdots \\ N_{k-1} &= 2q_k N_k + \varepsilon_{k+1} N_{k+1}, \end{aligned} \tag{264}$$

worin $N_1, N_2, \cdots N_{k+1}$ abnehmende positive ungerade Zahlen sind, deren letzte gleich 1 ist, $\varepsilon_1, \varepsilon_2, \cdots \varepsilon_{k+1}$ aber Einheiten bedeuten. Nun folgt aus einer Gleichung

$$N_{h-1} = 2q_h N_h + \varepsilon_{h+1} \cdot N_{h+1}$$

die andere:

$$\left(\frac{N_{h-1}}{N_h}\right) = \left(\frac{\varepsilon_{h+1} N_{h+1}}{N_h}\right) = \left(\frac{N_h}{N_{h+1}}\right) \cdot (-1)^{\frac{N_h - 1}{2} \cdot \frac{\varepsilon_{h+1} N_{h+1} - 1}{2}}$$

mithin, wenn diese Formel für $h = 0, 1, 2, \cdots k$ gebildet und dabei unter N_{-1} die Zahl M verstanden wird, durch Multiplikation der erhaltenen Gleichungen die Formel

$$\left(\frac{M}{N}\right) = (-1)^{\sum_{h=0}^{k} \frac{N_h - 1}{2} \cdot \frac{\varepsilon_{h+1} N_{h+1} - 1}{2}};$$

da aber in der Summe, welche den Exponenten von -1 bildet, jedes gerade Glied unterdrückt, jedes ungerade durch Eins ersetzt werden darf, so darf man statt der Summe die Anzahl der Fälle setzen, wo gleichzeitig N_h und $\varepsilon_{h+1} N_{h+1}$ von der Form $4z + 3$ sind, und erhält so folgende von Eisenstein (*J. f. Math.* 27, 1844, p. 317) gegebene Regel:

Man zähle, wie oft im Algorithmus (264) gleichzeitig N_h und $\varepsilon_{h+1} N_{h+1}$ (für $h = 0, 1, 2, \cdots k$) von der Form $4z + 3$ sind; ist λ diese Anzahl, so ist

$$\left(\frac{M}{N}\right) = (-1)^{\lambda}.$$

Statt lauter ungerader Reste kann man im Gegenteil lauter gerade Reste einführen, wenn man wieder positive und negative Reste zuläfst; denn, ist der Rest N_1 in der Formel (262) ungerade, so wird der Rest $N - N_1$ in der äquivalenten Formel (263) gerade sein. Wählt man also diejenige der beiden Formeln, in welcher der Rest gerade ist, bringt aber, bevor man weiter fortfährt, bei dem geraden Reste die höchste darin aufgehende Potenz von 2 zum Ausdruck u. s. w., so kann man statt des Algorithmus (264) folgenden andern aufstellen:

$$(265) \qquad \begin{aligned} M &= qN + 2^{m_1} \cdot \varepsilon_1 N_1 \\ N &= q_1 N_1 + 2^{m_2} \cdot \varepsilon_2 N_2 \\ &\cdots\cdots\cdots\cdots \\ N_{k-1} &= q_k N_k + 2^{m_{k+1}} \cdot \varepsilon_{k+1} N_{k+1}, \end{aligned}$$

wo die Zahlen $N_1, N_2, \cdots N_{k+1}$ wieder abnehmende positive, ungerade Zahlen sind, deren letzte gleich 1 ist, $\varepsilon_1, \varepsilon_2, \cdots \varepsilon_{k+1}$ Einheiten be-

deuten, k übrigens nicht dieselbe Zahl zu sein braucht wie in (264). Hier ist nun

$$\left(\frac{N_{h-1}}{N_h}\right) = \left(\frac{2^{m_{h+1}} \cdot \varepsilon_{h+1} N_{h+1}}{N_h}\right) = \left(\frac{N_h}{N_{h+1}}\right) \cdot \left(\frac{2}{N_h}\right)^{m_{h+1}} \cdot (-1)^{\frac{N_h - 1}{2} \cdot \frac{\varepsilon_{h+1} N_{h+1} - 1}{2}}$$

und es ergiebt sich wie zuvor:

$$\left(\frac{M}{N}\right) = (-1)^{\sum_{h=o}^{k} m_{h+1} \cdot \frac{N^2_h - 1}{8} + \sum_{h=o}^{k} \frac{N_h - 1}{2} \cdot \frac{\varepsilon_{h+1} N_{h+1} - 1}{2}},$$

eine Formel, aus der zufolge einer der obigen ähnlichen Überlegung sich nachstehende Regel ergiebt, die von **Lebesgue** (*Journ. de Math.* 12, 1847, p. 497) herrührt:

Man zähle, wie oft im Algorithmus (265) gleichzeitig N_h und $\varepsilon_{h+1} N_{h+1}$ (für $h = 0, 1, 2, \cdots k$) von der Form $4z + 3$ sind, und nenne diese Anzahl μ; man zähle ferner, wie oft darin gleichzeitig m_{h+1} ungerade und N_h von einer der Formen $8z + 3$, $8z + 5$ sind, und nenne diese Anzahl ν, dann ist

$$\left(\frac{M}{N}\right) = (-1)^{\mu + \nu}.$$

Lebesgue hat indessen noch eine zweite Regel (a. a. O.) gegeben. Man bilde nämlich für M, N den gewöhnlichen **Euclidischen** Algorithmus, bringe aber dabei in den einzelnen Resten die höchsten etwa darin aufgehenden Potenzen von 2 zum Ausdruck. Dann nimmt der Algorithmus nachstehende Form an:

$$\begin{aligned} M &= 2^{m_0} N \cdot q + 2^{m_1} N_1 \\ 2^{m_0} N &= 2^{m_1} N_1 \cdot q_1 + 2^{m_2} N_2 \\ &\cdots\cdots\cdots\cdots\cdots \\ 2^{m_{k-1}} N_{k-1} &= 2^{m_k} N_k \cdot q_k + 2^{m_{k+1}} N_{k+1}; \end{aligned} \tag{266}$$

wenn auch jetzt wieder M, N als ungerade vorausgesetzt werden, so ist $m_0 = 0$ und überhaupt $m_h = 0$ zu denken, wenn der h^{te} Rest ungerade ist; die Zahlen $N_1, N_2, \cdots N_{k+1}$ sind wieder abnehmende positive, ungerade Zahlen, deren letzte gleich 1 ist, und somit $m_{k+1} = 0$. Aus (266) ergiebt sich nun:

$$\left(\frac{2^{m_{h-1}}}{N_h}\right) \cdot \left(\frac{N_{h-1}}{N_h}\right) = \left(\frac{N_h}{N_{h+1}}\right) \cdot \left(\frac{2^{m_{h+1}}}{N_h}\right) \cdot (-1)^{\frac{N_h - 1}{2} \cdot \frac{N_{h+1} - 1}{2}}$$

mithin

$$\left(\frac{M}{N}\right) = (-1)^{\sum_{h=0}^{k} m_{h-1} \cdot \frac{N^2_h - 1}{8} + \sum_{h=0}^{k} m_{h+1} \cdot \frac{N^2_h - 1}{8} + \sum_{h=0}^{k} \frac{N_h - 1}{2} \cdot \frac{N_{h+1} - 1}{2}},$$

eine Formel, aus welcher sich, ähnlich wie oben, folgende neue Regel abliest:

Man zähle im Algorithmus (266), wie oft ein ungerades m_{h-1} mit einer Zahl N_h von einer der Formen $8z+3$, $8z+5$, und wie oft ein ungerades m_{h+1} mit einer derartigen Zahl N_h zusammentrifft, und nenne diese Anzahlen ϱ, σ; man zähle ferner, wie oft N_h, N_{h+1} gleichzeitig von der Form $4z+3$ sind, und nenne diese Anzahl τ, dann ist

$$\left(\frac{M}{N}\right) = (-1)^{\varrho+\sigma+\tau}.$$

Eine besonders elegante Regel gab **Kronecker** (*Berl. Sitzungsber.* 1884, p. 519 (530); vgl. dazu *Berl. Monatsber.* 1880, p. 698; s. auch Bachmann, *analyt. Zahlentheorie,* p. 169) und sie verdient vor den bisher betrachteten Bestimmungen auch insofern den Vorzug, als man dabei nicht auf positive Werte M, N beschränkt bleibt. Waren nämlich M, N beliebige, positive oder negative, aber relativ prime ungerade Zahlen, und δ, ε zwei solche Einheiten, dafs δM, εN positiv werden, so hatte man nach (60) mit leichter Änderung dieser Formel

$$(267)\qquad \left(\frac{M}{N}\right)\cdot\left(\frac{N}{M}\right) = (-1)^{\frac{M-1}{2}\cdot\frac{N-1}{2}-\frac{\delta-1}{2}\cdot\frac{\varepsilon-1}{2}}.$$

Nun seien n_0, n_1 zwei beliebige ungerade Zahlen ohne gemeinsamen Teiler, aus denen wir eine Reihe anderer Zahlen $n_2, n_3, n_4, \cdots$ in der Weise herleiten, dafs wir immer

$$(268)\qquad n_{h+1} = -2n_h\cdot R\left(\frac{n_{h-1}}{2n_h}\right)$$

wählen. Da, wenn g_h die nächste an $\frac{n_{h-1}}{2n_h}$ gelegene ganze Zahl bezeichnet,

$$R\left(\frac{n_{h-1}}{2n_h}\right) = \frac{n_{h-1}}{2n_h} - g_h$$

ist, so ergiebt sich

$$(269)\qquad 2n_h\cdot R\left(\frac{n_{h-1}}{2n_h}\right) = n_{h-1} - 2n_h g_h$$

d. i. die aus (268) bestimmte Zahl n_{h+1} ist eine **ganze** Zahl, sobald n_{h-1}, n_h schon ganze Zahlen sind, und da n_0, n_1 als solche vorausgesetzt sind, so besteht auch die Reihe der abgeleiteten Zahlen aus lauter ganzen, und zwar nach (268) aus absolut abnehmenden ganzen Zahlen, da $R\left(\frac{n_{h-1}}{2n_h}\right)$ absolut kleiner als $\frac{1}{2}$ ist. Zwischen drei aufeinanderfolgenden dieser Zahlen aber besteht die Gleichung (269), welche sich auch schreiben läfst, wie folgt:

$$(270)\qquad n_{h-1} - 2g_h n_h + n_{h+1} = 0.$$

Aus dieser Gleichung folgt, dafs, wie n_0, n_1, so auch je zwei aufeinanderfolgende Zahlen n_h, n_{h+1} ohne gemeinsamen Teiler sind, und da die n_h abnehmen, mufs somit eine letzte Zahl n_{k+1} vorhanden sein, deren Wert ± 1 ist. Nun giebt die Gleichung (270) weiter für das Symbol $\left(\frac{n_{h-1}}{-n_h}\right) = \left(\frac{n_{h-1}}{n_h}\right)$ die Beziehung

$$\left(\frac{-n_{h+1}}{n_h}\right) = \left(\frac{n_{h-1}}{-n_h}\right)$$

woraus

$$\prod_{h=1}^{k}\left(\frac{-n_{h+1}}{n_h}\right) = \prod_{h=1}^{k}\left(\frac{n_{h-1}}{-n_h}\right)$$

hervorgeht. Dieser Gleichung giebt man leicht die Form:

$$\left(\frac{-n_1}{n_0}\right)\cdot\prod_1^{k+1}\left(\frac{-n_h}{n_{h-1}}\right) = \left(\frac{n_k}{-n_{k+1}}\right)\cdot\prod_1^{k+1}\left(\frac{n_{h-1}}{-n_h}\right),$$

in welcher wegen $n_{k+1} = \pm 1$ das Symbol $\left(\frac{n_k}{-n_{k+1}}\right) = 1$ ist. Wird diese Formel beiderseits mit dem links stehenden Produkte multipliziert, so findet sich einfach

$$\left(\frac{-n_1}{n_0}\right) = \prod_1^{k+1}\left(\frac{-n_h}{n_{h-1}}\right)\left(\frac{n_{h-1}}{-n_h}\right).$$

Nun führe man Einheiten ε_h, η_h ein durch die Bedingungen, dafs $\varepsilon_h n_h$ positiv und $\eta_h n_h \equiv 1 \pmod{4}$ werde. Dann geht die vorstehende Formel mit Rücksicht auf die allgemeine Formel (267) in die neue Gestalt:

$$\left(\frac{-n_1}{n_0}\right) = (-1)^{\frac{\sigma}{4}}$$

über, worin

$$\sigma = \sum_{h=1}^{k+1}\left[(\eta_{h-1}-1)(\eta_h+1) - (\varepsilon_{h-1}-1)(\varepsilon_h+1)\right]$$

zu setzen ist. Diese Summe aber vereinfacht sich leicht zu dem folgenden Ausdruck

$$\eta_0 - \eta_{k+1} - \varepsilon_0 + \varepsilon_{k+1} + \sum_{h=1}^{k+1}(\eta_{h-1}\eta_h - \varepsilon_{h-1}\varepsilon_h),$$

wo wegen $n_{k+1} = \pm 1$ sich ε_{k+1} gegen η_{k+1} weghebt. Setzt man demnach noch

$$n_{-1} = 1,\ \varepsilon_{-1} = 1,\ \eta_{-1} = 1,$$

so kann man schreiben

$$\sigma = \sum_{h=0}^{k+1} (\eta_{h-1}\eta_h - \varepsilon_{h-1}\varepsilon_h),$$

woraus sich sogleich nachstehende zwei Formeln ergeben:

$$\frac{\sigma}{2} = \sum_{h=0}^{k+1} \frac{1+\eta_{h-1}\eta_h}{2} - \sum_{h=0}^{k+1} \frac{1+\varepsilon_{h-1}\varepsilon_h}{2}$$

$$\frac{\sigma}{2} = \sum_{h=0}^{k+1} \frac{1-\varepsilon_{h-1}\varepsilon_h}{2} - \sum_{h=0}^{k+1} \frac{1-\eta_{h-1}\eta_h}{2}.$$

Nun ist

$$\frac{1+\varepsilon_{h-1}\varepsilon_h}{2} = 0 \text{ oder } 1, \text{ bezw. } \frac{1-\varepsilon_{h-1}\varepsilon_h}{2} = 1 \text{ oder } 0,$$

jenachdem beim Übergange von n_{h-1} zu n_h ein Zeichenwechsel eintritt oder nicht, und ähnliches gilt für $\frac{1 \pm \eta_{h-1}\eta_h}{2}$. Man findet hiernach ohne Mühe die Regel, welche **Kronecker** ausgesprochen hat, nämlich folgenden Satz:

Man bestimme für die nach obiger Vorschrift gebildete Zahlenreihe

$$1,\ n_0,\ n_1,\ n_2, \cdots n_k,\ \pm 1$$

die Anzahl φ der Folgen und die Anzahl φ' der Wechsel ihrer Vorzeichen, sowie die Anzahl ψ der Folgen und die Anzahl ψ' der Wechsel der Vorzeichen ihrer absolut kleinsten Reste (mod. 4), so ist

$$\left(\frac{-n_1}{n_0}\right) = (-1)^{\frac{\psi-\varphi}{2}} = (-1)^{\frac{\psi'-\varphi'}{2}}. \tag{271}$$

Auf eine andere bemerkenswerte Formulierung, welche Kronecker (a. a. O.) dieser Regel noch gegeben hat, sei hier nur hingewiesen.

Sehr ähnlich ist die Regel, welche schon etwas früher von Sylvester (*Par. C. R.* 90, 1880, p. 1053) gegeben worden ist. Diese stützt sich auf den Algorithmus

$$n_0 = 2g_1 n_1 + n_2$$
$$n_1 = 2g_2 n_2 + n_3$$
$$\cdots\cdots\cdots$$
$$n_{k-1} = 2g_k n_k + n_{k+1},$$

dem gemäfs die sämtlichen n_i positive oder negative, aber, wie n_0, n_1 ungerade Zahlen sind, die letzte $n_{k+1} = \pm 1$, wenn n_0, n_1 als relativ prim vorausgesetzt werden. Ganz wie bei Kronecker findet sich

aus diesem Algorithmus, unter Beibehaltung der bisherigen Bezeichnungen

$$\left(\frac{n_1}{n_0}\right) = (-1)^\tau,$$

worin

$$\tau = \sum_{h=1}^{k+1}\left(\frac{n_{h-1}-1}{2}\cdot\frac{n_h-1}{2} - \frac{\varepsilon_{h-1}-1}{2}\cdot\frac{\varepsilon_h-1}{2}\right)$$

$$\equiv \sum_{h=1}^{k+1}\left(\frac{\eta_{h-1}-1}{2}\cdot\frac{\eta_h-1}{2} + \frac{\varepsilon_{h-1}-1}{2}\cdot\frac{\varepsilon_h-1}{2}\right) \pmod{2}.$$

Bemerkt man aber, dafs das Glied

$$\frac{\eta_{h-1}-1}{2}\cdot\frac{\eta_h-1}{2} \text{ resp. } \frac{\varepsilon_{h-1}-1}{2}\cdot\frac{\varepsilon_h-1}{2}$$

nur dann nicht verschwindet, sondern den Beitrag 1 zur Summe liefert, wenn η_{h-1}, η_h resp. ε_{h-1}, ε_h eine negative Zeichenfolge bilden also zugleich den Wert -1 haben, so erschliefst man die Sylvestersche Regel:

Ist α die Anzahl der negativen Zeichenfolgen in der Reihe

$$n_0, n_1, n_2, \cdots n_{k+1},$$

β die Anzahl dieser Zeichenfolgen in der Reihe ihrer absolut kleinsten Reste (mod. 4), so ist

$$\left(\frac{n_1}{n_0}\right) = (-1)^{\alpha+\beta}.$$

Während bei diesen beiden Regeln nur ungerade Reste benutzt werden, hat Gegenbauer (*Wiener Ber.* 82 II, 1880, p. 931; 84 II, 1881, p. 1089) Algorithmen verwendet, bei denen ungerade und gerade Reste abwechseln. Er entwickelt nämlich $\frac{-2n_1}{n_0}$ bezw. $\frac{n_0}{2n_1}$ in Kettenbrüche mit geraden Teilnennern und den Teilzählern -1; die daraus entspringenden Regeln haben analogen Charakter, wie die von Kronecker und von Sylvester, doch insofern einen Vorzug vor diesen voraus, als bei ihnen es der Untersuchung nicht zweier, sondern nur einer Zahlenreihe in Bezug auf ihre Zeichen-Folgen und -Wechsel bedarf.

Schliefslich sei hier noch die elegante Form hervorgehoben, welche Sylvester a. a. O. dem allgemeinen Reziprozitätsgesetze gegeben hat, indem er ein Zeichen

$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$$

einführt mit der Bedeutung, gleich -1 zu sein, wenn a, b gleichzeitig negativ sind, andernfalls gleich $+1$. Sind nämlich M', N'

die absolut kleinsten Reste der Zahlen M, N (mod. 4), so läſst sich dann die Formel (267) offenbar folgendermaſsen schreiben:

$$\left(\frac{M}{N}\right)\cdot\left(\frac{N}{M}\right)=\left(\frac{M}{N}\right)\cdot\left(\frac{M'}{N'}\right). \tag{267a}$$

30. Wenn p eine ungerade Primzahl bedeutet, so giebt es, wie in Nr. 2 gezeigt worden, ebensoviel quadratische Reste als Nichtreste von p, oder die Zahlen $1, 2, 3, \cdots p-1$ zerfallen in $\frac{p-1}{2}$ quadr. Reste, welche a, und in $\frac{p-1}{2}$ quadr. Nichtreste, welche b heiſsen mögen. Es ist nicht ohne Interesse zu untersuchen, wie diese Reste oder Nichtreste sich über das Intervall o bis p verteilen. Wir wollen das letztere in die vier kleineren Intervalle

$$o, \frac{p}{4}; \ \frac{p}{4}, \frac{p}{2}; \ \frac{p}{2}, \frac{3p}{4}; \ \frac{3p}{4}, p$$

zerlegen und nennen A_1, A_2, A_3, A_4, resp. B_1, B_2, B_3, B_4 die Anzahl der quadratischen Reste bezw. Nichtreste von p in diesen einzelnen Teilintervallen; auch seien für das i^{te} Intervall A_i', A_i'', bezw. B_i', B_i'' die Anzahl der darin enthaltenen geraden und ungeraden quadr. Reste resp. Nichtreste, sodaſs

$$A_i' + A_i'' = A_i, \quad B_i' + B_i'' = B_i \tag{272}$$

ist.

Wenn nun zuerst $p = 4z+1$ also -1 quadr. Rest von p ist, so sind $a, p-a$ quadratische Reste, einer kleiner, der andere gröſser als $\frac{p}{2}$, einer gerade, der andere ungerade. Hieraus folgt, daſs die Anzahl quadratischer Reste, welche $<\frac{p}{2}$, gleich der Anzahl derjenigen ist, welche $>\frac{p}{2}$ sind, sowie daſs die Anzahl der geraden und der ungeraden quadratischen Reste $<\frac{p}{2}$ gleich der Anzahl der ungeraden resp. der geraden quadratischen Reste $>\frac{p}{2}$ ist, mithin die Anzahl der geraden derjenigen der ungeraden gleichkommt, Sätze, welche in den Gleichungen:

$$\left\{\begin{aligned} A_1 + A_2 &= A_3 + A_4 = \frac{p-1}{4} \\ A_1' + A_2' &= A_3'' + A_4'' \\ A_1'' + A_2'' &= A_3' + A_4' \end{aligned}\right. \tag{273}$$

sowie in der aus den beiden letzten folgenden Gleichung

$$A_1' + A_2' + A_3' + A_4' = A_1'' + A_2'' + A_3'' + A_4'' = \frac{p-1}{4} \tag{274}$$

ihren formalen Ausdruck finden. — Da ferner, wenn $a < \frac{p}{4}$ ist, $p - a > \frac{3p}{4}$ ist, und umgekehrt, so findet man genauer folgende Beziehungen:

$$(275)\quad \begin{cases} A_1 = A_4, \quad A_2 = A_3 \\ A_1' = A_4'', \quad A_1'' = A_4', \quad A_2' = A_3'', \quad A_2'' = A_3', \end{cases}$$

aus denen die voraufgehenden wieder geschlossen werden können. Entsprechendes gilt in diesem Falle von den quadratischen Nichtresten.

Da jedes Paar $a, p - a$ quadratischer Reste, sowie jedes Paar $b, p - b$ quadratischer Nichtreste die Summe p hat, und $\frac{p-1}{4}$ solcher Paare jeder Art vorhanden sind, so ist in diesem Falle die Summe der quadratischen Reste ebenso wie die Summe der quadratischen Nichtreste gleich $p \cdot \frac{p-1}{4}$, in Zeichen:

$$(276)\quad \sum a = \sum b = \frac{p-1}{4} p.$$

Ist dagegen zweitens $p = 4z + 3$ also -1 quadratischer Nichtrest von p, so sind $a, p - a$ sowie $b, p - b$ von verschiedenem quadratischen Charakter. Also giebt es in diesem Falle soviel gerade (ungerade) quadratische Reste $< \frac{p}{2}$, als es ungerade (gerade) quadratische Nichtreste $> \frac{p}{2}$ giebt, und soviel gerade (ungerade) quadratische Nichtreste $< \frac{p}{2}$, als ungerade (gerade) quadratische Reste $> \frac{p}{2}$, in Zeichen:

$$(277)\quad \begin{cases} A_1' + A_2' = B_3'' + B_4'' \\ A_1'' + A_2'' = B_3' + B_4' \\ B_1' + B_2' = A_3'' + A_4'' \\ B_1'' + B_2'' = A_3' + A_4'. \end{cases}$$

Die Anzahl der geraden quadratischen Reste (Nichtreste) ist mithin gleich derjenigen der ungeraden quadratischen Nichtreste (Reste), wie die aus (277) gefolgerten Gleichungen:

$$(278)\quad \begin{cases} A_1' + A_2' + A_3' + A_4' = B_1'' + B_2'' + B_3'' + B_4'' \\ B_1' + B_2' + B_3' + B_4' = A_1'' + A_2'' + A_3'' + A_4'' \end{cases}$$

besagen. Aus dem Umstande, dafs, wenn α im ersten oder zweiten der vier Teilintervalle liegt, $p - \alpha$ im vierten resp. im dritten derselben enthalten ist, und umgekehrt, folgen genauer die Beziehungen:

$$(279)\quad A_1 = B_4, \quad B_1 = A_4, \quad A_2 = B_3, \quad B_2 = A_3$$

sowie

$$(280)\quad \begin{cases} A_1' = B_4'', \quad A_1'' = B_4', \quad B_1' = A_4'', \quad B_1'' = A_4', \\ A_2' = B_3'', \quad A_2'' = B_3', \quad B_2' = A_3'', \quad B_2'' = A_3'. \end{cases}$$

In diesem Falle ist offenbar $\sum b = \sum (p-a)$ d. i., da die Anzahl der Zahlen a gleich $\frac{p-1}{2}$ ist,

$$(281) \qquad \sum a + \sum b = p \cdot \frac{p-1}{2},$$

eine Formel, die übrigens auch im vorigen Falle wegen (276) richtig ist und in der That bestehen mufs, da die Zahlen a, b zusammengenommen die Reihe der Zahlen $1, 2, 3, \cdots p-1$ erschöpfen. In demselben Falle bestehen aber zwischen den Anzahlen A_i, B_i noch weitere Beziehungen, die zuerst von Lebesgue (*Journ. de Math.* 7, 1842, p. 137), sodann auf einfachere Weise von Götting (*Journ. f. Math.* 70, 1869, p. 363) und von Stern (ebend. 71, 1870, p. 137) bewiesen worden sind.

Man bemerke dazu einerseits, dafs die mit 2 multiplizierten Zahlen des ersten Teilintervalls die geraden Zahlen zwischen 0 und $\frac{p}{2}$, die doppelt genommenen Zahlen des dritten Intervalles aber die geraden Zahlen zwischen p und $\frac{3p}{2}$ sind, deren Reste (mod. p) mit den ungeraden Zahlen zwischen 0 und $\frac{p}{2}$ übereinstimmen, dafs mithin die doppelt genommenen Zahlen des ersten und dritten Intervalles den Zahlen des ersten und zweiten kongruent sind; bedenkt man dann andererseits, dafs, jenachdem p von der Form $8z+7$ oder $8z+3$ ist, 2 quadratischer Rest oder Nichtrest von p ist, also die doppelt genommenen Zahlen denselben bezw. den entgegengesetzten quadratischen Charakter haben, wie die einfachen, so finden sich sogleich,

wenn p von der Form $8z+3$ ist, die Beziehungen

$$A_1 + A_3 = B_1 + B_2, \quad B_1 + B_3 = A_1 + A_2,$$

aus denen wegen (279)

$$(282) \qquad A_1 = B_1$$

d. i. der Satz hervorgeht, dafs in diesem Falle zwischen 0 und $\frac{p}{4}$ ebensoviel quadratische Reste als Nichtreste enthalten sind, nämlich $z = \frac{p-3}{8}$;

wenn aber p von der Form $8z+7$ ist, so wird

$$A_1 + A_3 = A_1 + A_2, \quad B_1 + B_3 = B_1 + B_2$$

mithin

$$(283) \qquad A_2 = A_3, \quad B_2 = B_3$$

d. h. zwischen $\frac{p}{4}$ und $\frac{p}{2}$ liegen ebensoviel quadratische Reste (Nicht-

reste), wie zwischen $\frac{p}{2}$ und $\frac{3p}{4}\cdot$ Nach (279) lassen sich diese Gleichungen aber auch schreiben, wie folgt:

(284) $$A_2 = B_2, \quad A_3 = B_3$$

und folglich ist in jedem dieser Intervalle die Anzahl der quadratischen Reste gleich derjenigen der Nichtreste.

Der ersten der vorigen Gleichungen zufolge ist für eine Primzahl p von der Form $8z+7$, da für eine solche 2 quadratischer Rest ist, die Anzahl der Nichtreste zwischen $\frac{p}{4}$ und $\frac{p}{2}$ auch gleich der Anzahl der geraden quadratischen Reste zwischen $\frac{p}{2}$ und p, d. i. gleich derjenigen der ungeraden Nichtreste zwischen 0 und $\frac{p}{2}\cdot$ Dieser Satz besteht auch für Primzahlen von der Form $8z+1$; denn in diesem Falle war die Anzahl der ungeraden quadratischen Nichtreste zwischen 0 und $\frac{p}{2}$ gleich derjenigen der geraden Nichtreste zwischen $\frac{p}{2}$ und p und ist also, da 2 quadratischer Rest von p ist, der Anzahl der Nichtreste zwischen $\frac{p}{4}$ und $\frac{p}{2}$ gleich. Nimmt man nun beiderseits die ungeraden Nichtreste zwischen $\frac{p}{4}$ und $\frac{p}{2}$ weg, so findet sich die Anzahl der ungeraden Nichtreste zwischen 0 und $\frac{p}{4}$ gleich derjenigen der geraden Nichtreste zwischen $\frac{p}{4}$ und $\frac{p}{2}$ d. i. gleich der Anzahl der Nichtreste zwischen $\frac{p}{8}$ und $\frac{p}{4}\cdot$ Setzt man diese Betrachtung in gleicher Weise fort, so gelangt man allgemeiner zu dem von Stern angegebenen Resultate: Für Primzahlen p von einer der Formen $8z+1$ oder $8z+7$ giebt es ebensoviel ungerade quadratische Nichtreste zwischen 0 und $\frac{p}{2^m}$, als Nichtreste überhaupt zwischen $\frac{p}{2^{m+1}}$ und $\frac{p}{2^m}\cdot$

Andere hierhergehörige Sätze gab Dirichlet, doch gewann er sie aus Betrachtungen ungleich höherer Art, die hier nicht reproduziert werden können, nämlich aus seinen auf analytischem Wege gefundenen Formeln für die sogenannte Klassenanzahl quadratischer Formen, und sie sind auch bisher noch nicht auf andere Weise bestätigt worden. Aus jenen Formeln schliefst man u. a., dafs für Primzahlen p von der Form $4z+1$

(285) $$A_1 > B_1$$

ist; da nun $A_1 + B_1 = \frac{p-1}{4} = z$, so folgt $2A_1 - z > 0$.

Desgleichen ist für Primzahlen p von der Form $4z+3$

(286) $$A_1 + A_2 > B_1 + B_2,$$

dagegen, wenn die Summen auf alle quadratischen Reste resp. Nichtreste (mod. p) bezogen werden,

(287) $$\sum a < \sum b;$$

es ist nämlich

(288) $$A_1 + A_2 - (B_1 + B_2) = \left(2 - \left(\frac{2}{p}\right)\right) \cdot \frac{\Sigma b - \Sigma a}{p}$$

gleich einer positiven ganzen Zahl. Wenn nun z gerade d. h. $p \equiv 3 \pmod{8}$, so ist nach (282) $A_1 = B_1$ also $2A_1 = A_1 + B_1 = \frac{p-3}{4} = z$, mithin $2A_1 - z = 0$. Ist aber z ungerade d. i. $p \equiv 7 \pmod{8}$, so folgt aus (286) wegen (284) $A_1 > B_1$ also $2A_1 > A_1 + B_1 = \frac{p-3}{4} = z$, mithin $2A_1 - z > 0$.

Stern hat (a. a. O.) diese und noch andere Dirichletsche Sätze benutzt, um die Verteilung der quadratischen Reste und Nichtreste noch genauer zu ermitteln. Wir beschränken uns in Wiedergabe seiner Ergebnisse auf den Fall der Primzahlen $p = 4z + 1$. Nach (273), (274) hat man in diesem Falle

$$A_1' + A_2' + A_1'' + A_2'' = \frac{p-1}{4};$$

da aber die geraden quadratischen Reste und Nichtreste, welche $< \frac{p}{2}$, die sämtlichen geraden Zahlen $< \frac{p}{2}$ ausmachen, deren Anzahl $\frac{p-1}{4}$ ist, findet sich ferner

$$A_1' + A_2' + B_1' + B_2' = \frac{p-1}{4}$$

mithin

(289) $$A_1'' + A_2'' = B_1' + B_2'$$

und ähnlich

(290) $$A_1' + A_2' = B_1'' + B_2''.$$

Ist nun zunächst z gerade d. i. $p \equiv 1 \pmod{8}$, so ist die Anzahl der geraden quadratischen Reste (Nichtreste) zwischen 0 und $\frac{p}{2}$ gleich derjenigen der quadratischen Reste (Nichtreste) zwischen 0 und $\frac{p}{4}$ d. h.

$$A_1' + A_2' = A_1, \quad B_1' + B_2' = B_1$$

und folglich

(291) $$A_2' = A_1'', \quad B_2' = B_1''.$$

Die Ungleichheit (285) nimmt demnach die Form an

$$A_1' + A_2' > B_1' + B_2'$$

oder wegen (289)

$$A_1' + A_2' > A_1'' + A_2''$$

d. h. es giebt in diesem Falle zwischen 0 und $\frac{p}{2}$ mehr gerade als ungerade quadratische Reste; wegen (291) folgt

(292) $$A_1' > A_2''.$$

Ist dagegen z ungerade also $p \equiv 5 \pmod{8}$, so findet sich in analoger Weise

$$A_1' + A_2' = B_1, \quad B_1' + B_2' = A_1$$

d. i.

$$A_1' + A_2' = B_1'' + B_2'' = B_1' + B_1'',$$

$$B_1' + B_2' = A_1'' + A_2'' = A_1' + A_1''$$

also

(293) $$B_1' = B_2'', \quad A_1' = A_2''$$

und die Ungleichheit (285) nimmt die Form an

$$B_1' + B_2' > A_1' + A_2'$$

d. i. wegen (289)

$$A_1'' + A_2'' > A_1' + A_2'$$

und folglich giebt es umgekehrt in diesem Falle zwischen 0 und $\frac{p}{2}$ mehr ungerade als gerade quadratische Reste.

Was so für das Intervall 0 bis $\frac{p}{2}$ bewiesen ist, läſst sich gleicherweise als für das Intervall 0, $\frac{p}{4}$ giltig erweisen, wenn man sich eines weiteren der Dirichletschen Sätze bedient. Bedeuten nämlich A, A' die Anzahl quadratischer Reste, B, B' diejenige der quadratischen Nichtreste zwischen 0 und $\frac{p}{8}$ resp. zwischen $\frac{3p}{8}$ und $\frac{p}{2}$, so ist nach den Dirichletschen Formeln

$$A - A' > B - B'.$$

Ist nun zuerst $p \equiv 1 \pmod{8}$, so ist offenbar

$$A = A_1', \quad B = B_1', \quad A' = A_4', \quad B' = B_4'$$

also

$$A_1' + B_4' > B_1' + A_4',$$

oder, da nach (275) $A_4' = A_1''$ und ebenso $B_4' = B_1''$ ist,

$$A_1' + B_1'' > A_1'' + B_1'$$

folglich

$$2A_1' + A_1'' + B_1'' > 2A_1'' + A_1' + B_1'$$

oder, da $A_1' + B_1'$ bezw. $A_1'' + B_1''$ die Anzahl aller geraden resp. ungeraden Zahlen $< \frac{p}{4}$ also

$$A_1' + B_1' = A_1'' + B_1'' = \frac{p-1}{8}$$

ist,

$$A_1' > A_1'',$$

und demnach liegen in diesem Falle zwischen 0 und $\frac{p}{4}$ mehr gerade als ungerade quadratische Reste. Wegen (291) schliefst man ferner $A_1' > A_2'$, daher giebt es in diesem Falle zwischen 0 und $\frac{p}{4}$ mehr gerade quadratische Reste als zwischen $\frac{p}{4}$ und $\frac{p}{2}$ oder auch, da 2 quadratischer Rest ist, mehr quadratische Reste überhaupt zwischen 0 und $\frac{p}{8}$ als zwischen $\frac{p}{8}$ und $\frac{p}{4}$.

Ist dagegen zweitens $p \equiv 5 \pmod{8}$, so findet sich ähnlicherweise

$$A = B_1', \quad B = A_1', \quad A' = B_4', \quad B' = A_4'$$

also

$$B_1' + A_4' > A_1' + B_4',$$

oder wegen (275)

$$B_1' + A_1'' > A_1' + B_1''$$

folglich

$$B_1' + A_1' + 2A_1'' > 2A_1' + A_1'' + B_1''.$$

Hier ist $A_1' + B_1'$ die Anzahl aller geraden Zahlen $< \frac{p}{4}$ also gleich $\frac{p-5}{8}$, ebenso $A_1'' + B_1''$ die Anzahl aller ungeraden Zahlen $< \frac{p}{4}$ also gleich $\frac{p+3}{8}$, mithin gröfser als jene; aus der vorigen Ungleichheit folgt also

$$A_1'' > A_1'$$

und daher giebt es im gegenwärtigen Falle zwischen 0 und $\frac{p}{4}$ mehr ungerade als gerade quadratische Reste. Da in demselben Falle wegen (293) sich $A_1'' > A_2''$ also nach (275) sich $A_4' > A_3'$ ergiebt, so schliefst man endlich noch, dafs es in ihm zwischen $\frac{3p}{4}$ und p mehr gerade quadratische Reste giebt als zwischen $\frac{p}{2}$ und $\frac{3p}{4}$, oder auch, da 2 quadratischer Nichtrest ist, dafs zwischen $\frac{3p}{8}$ und $\frac{p}{2}$ mehr quadratische Nichtreste vorhanden sind, als zwischen $\frac{p}{4}$ und $\frac{3p}{8}$.

Der Fall einer Primzahl p von der Form $4z + 3$ bietet ähnliche Sätze dar, von denen wir aber nur den einen anmerken wollen, dafs, wenn z gerade also $p \equiv 3 \pmod{8}$ ist, zwischen $\frac{p}{4}$ und $\frac{3p}{8}$ immer mehr quadratische Reste enthalten sind, als zwischen 0 und $\frac{p}{8}$.

31. Wir wollen nun mit Stern (*Journ. f. Math.* 69, 1868, p. 370) die Reste betrachten, welche die sogenannten Trigonalzahlen d. h. die Zahlen von der Form

$$\frac{x(x+1)}{2},$$

durch eine ungerade Primzahl p geteilt, lassen. Die von Null verschiedenen dieser Reste (oder jedes System ihnen kongruenter Zahlen) sollen die **trigonalen Reste** (mod. p) heifsen. Da die Kongruenz

$$\frac{x(x+1)}{2} \equiv \frac{y(y+1)}{2} \pmod{p}$$

mit der anderen:

$$(y-x)(y+x+1) \equiv 0 \pmod{p}$$

gleichbedeutend ist, so kann sie nur stattfinden, wenn entweder $y \equiv x$ oder $y \equiv -x-1 \pmod{p}$ ist. Um die verschiedenen, nämlich inkongruenten trigonalen Reste zu erhalten, braucht man mithin in $\frac{x(x+1)}{2}$ für x nur die Zahlen $0, 1, 2, 3, \cdots p-1$ zu setzen, und je zwei von ihnen: x und $p-x-1$, welche von einander verschieden sind, aufser wenn $x = \frac{p-1}{2}$ ist, entspricht der gleiche trigonale Rest; für $x = \frac{p-1}{2}$ erhält man das isoliert stehende Mittelglied $\frac{p^2-1}{8}$, dessen Rest M genannt werden soll; für $x = 0$ und $x = p-1$ erhält man den Rest 0. Demnach giebt die Formel $\frac{x(x+1)}{2}$ die verschiedenen trigonalen Reste, wenn darin $x = 1, 2, 3, \cdots \frac{p-1}{2}$ gesetzt wird, mithin ist ihre Anzahl gleich $\frac{p-1}{2}$. Die übrigen $\frac{p-1}{2}$ Zahlen der Reihe $1, 2, 3, \cdots p-1$ sind die **trigonalen Nichtreste**.

1) Da $M \equiv \frac{p^2-1}{8} \pmod{p}$, so ist $8M+1 \equiv 0 \pmod{p}$. Für jeden von M verschiedenen trigonalen Rest m aber, d. h. für jede von M verschiedene Zahl m der Reihe $1, 2, 3, \cdots p-1$, für welche die Kongruenz $\frac{x(x+1)}{2} \equiv m \pmod{p}$ möglich ist, findet sich

$$(2x+1)^2 \equiv 8m+1 \pmod{p}, \tag{294}$$

ist also $8m+1$ ein quadratischer Rest (mod. p). Für jeden trigonalen Nichtrest m dagegen ist $8m+1$ ein quadratischer Nichtrest (mod. p); denn, wäre das Gegenteil der Fall also $y^2 \equiv 8m+1 \pmod{p}$, so könnte man, da mit y zugleich auch $p-y$ eine Wurzel der letzteren Kongruenz wäre, y ungerade voraussetzen und erhielte die Kongruenz (294), welcher die andere:

$$\frac{x(x+1)}{2} \equiv m \pmod{p} \tag{295}$$

gleichbedeutend ist, d. h. m wäre ein trigonaler Rest, gegen Voraussetzung. Setzt man in Analogie mit dem **Legendreschen** Symbole

das Zeichen $\left(\frac{m}{=p}\right)$ gleich $+1$ oder -1, jenachdem m trigonaler Rest oder Nichtrest von p ist, so findet sich hiernach,

(296) wenn $m \gtrless M$ ist, $\left(\frac{m}{=p}\right) = \left(\frac{8m+1}{p}\right)$.

Nun durchläuft der Ausdruck $8m+1$ ein vollständiges Restsystem (mod. p), wenn m ein solches durchläuft; man erhält mithin sämtliche von 1 verschiedene quadratische Reste (mod. p), wenn man in $8m+1$ für m die trigonalen Reste $m \gtrless M$ setzt, sowie sämtliche quadratischen Nichtreste, wenn man darin für m die sämtlichen trigonalen Nichtreste (mod. p) setzt.

Da $8M \equiv -1$ (mod. p) also $8 \cdot 2M + 1 \equiv -1$ ist, so mufs hiernach $2M$ trigonaler Rest oder Nichtrest sein, jenachdem -1 quadratischer Rest oder Nichtrest d. i. jenachdem p von der Form $4z+1$ oder $4z+3$ ist; der Kongruenz $8M \equiv -1$ zufolge ist aber $2M$ jenach diesen beiden Fällen auch quadratischer Rest oder Nichtrest, und somit ergiebt sich die Beziehung

(297) $$\left(\frac{2M}{=p}\right) = \left(\frac{2M}{p}\right).$$

2) Untersuchen wir allgemeiner, ob eine Zahl m zugleich trigonaler und quadratischer Rest sein kann. Ist aber zugleich

$$\frac{x(x+1)}{2} \equiv m, \quad y^2 \equiv m \pmod{p},$$

wobei $x, y < \frac{p}{2}$ gedacht werden können, so ergiebt sich

$$(2x+1)^2 \equiv 8y^2 + 1 \pmod{p}$$

oder, indem man

(298) $$X = 2x + 1, \quad Y = 2y$$

setzt, die Kongruenz

(299) $$X^2 - 2Y^2 \equiv 1 \pmod{p}.$$

Nun hat eine Kongruenz

$$a_1 X^2 + a_2 Y^2 \equiv \alpha \pmod{p},$$

in welcher a_1, a_2, α ganze Zahlen sind, deren letzte durch p nicht teilbar ist, $p - \left(\frac{-a_1 a_2}{p}\right)$ inkongruente Auflösungen X, Y (s. Libri, *Journ. f. Math.* 9, 1832, p. 183 oder des Verfassers *Arithmetik der quadratischen Formen*, 1898, p. 489); daher ist die Anzahl aller solcher Auflösungen X, Y für die Kongruenz (299) gleich $p - \left(\frac{2}{p}\right)$; von ihnen sind aber zufolge (298) nur diejenigen beizubehalten, bei denen X eine ungerade, Y eine von Null verschiedene gerade Zahl ist. Daher sind die beiden evidenten Lösungen $X = \pm 1, Y = 0$ auszuschliefsen und es bleiben zur Betrachtung nur noch $p - 2 - \left(\frac{2}{p}\right)$.

Ist nun zunächst $p = 8z + 1$, so ist die Kongruenz $-2Y^2 \equiv 1 \pmod{p}$ möglich und hat zwei Wurzeln η, $p - \eta$, deren eine gerade ist; dem entsprechen zwei Lösungen der Kongruenz (299):

$$X = p,\ y = \eta;\quad X = p,\ Y = p - \eta,$$

von denen eine hier zulässig ist. Bei allen übrigen $p - 4 - \left(\frac{2}{p}\right) = p - 5 = 8z - 4$ Lösungen sind X, Y durch p nicht teilbar; jeder dieser Lösungen gehören also noch drei andere: $X, p - Y$; $p - X, Y$; $p - X, p - Y$ zu und von diesen je vier zusammengehörigen Lösungen ist offenbar nur eine zulässig, nämlich so beschaffen, dafs das erste Element ungerade, das zweite gerade ist. Im ganzen giebt es also $1 + (2z - 1) = 2z$ zulässige Auflösungen der Kongruenz (299) und entsprechende Werte von m, d. h. von den $\frac{p-1}{2} = 4z$ trigonalen Resten sind in diesem Falle ebensoviele quadratische Reste als Nichtreste.

Ist zweitens $p = 8z + 3$, so ist die Kongruenz $-2Y^2 \equiv 1 \pmod{p}$ ebenfalls möglich und ergiebt eine zulässige Lösung von (299). Bezüglich der übrigen $p - 4 - \left(\frac{2}{p}\right) = p - 3 = 8z$ Lösungen gilt aber genau das soeben Bemerkte, und man erhält also $1 + 2z$ zulässige Lösungen d. h. unter den $\frac{p-1}{2} = 4z + 1$ trigonalen Resten befindet sich in diesem Falle ein quadratischer Rest mehr als quadratische Nichtreste.

In den beiden anderen möglichen Fällen $p = 8z + 5$, $p = 8z + 7$ ist die Kongruenz $-2Y^2 \equiv 1 \pmod{p}$ nicht lösbar.

Ist demnach jetzt $p = 8z + 5$, so ist von den zu betrachtenden $p - 2 - \left(\frac{2}{p}\right) = p - 1 = 8z + 4$ Lösungen nur der vierte Teil, also $2z + 1$ Lösungen zulässig, mithin giebt es unter den $\frac{p-1}{2} = 4z + 2$ trigonalen Resten in diesem Falle wieder, wie im ersten, gleichviel quadratische Reste und quadratische Nichtreste.

Ist aber endlich $p = 8z + 7$, so sind von jenen $p - 2 - \left(\frac{2}{p}\right) = p - 3 = 8z + 4$ Lösungen wieder nur $2z + 1$ zulässig, und folglich giebt es in diesem Falle unter den $\frac{p-1}{2} = 4z + 3$ trigonalen Resten einen quadratischen Rest weniger als quadratische Nichtreste.

3) Setzt man in (296) die von 0 und M verschiedene Zahl m gleich $2M - n$, sodafs n von M und $2M$ verschieden ist, so folgt

$$\left(\frac{2M - n}{p}\right) = \left(\frac{16M - 8n + 1}{p}\right)$$

d. i. wegen $8M + 1 \equiv 0 \pmod{p}$

$$\left(\frac{2M - n}{p}\right) = \left(\frac{-8n - 1}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{8n + 1}{p}\right);$$

da aber $n \gtrless M$, so nimmt diese Formel nach (296) die Gestalt an:

$$(300) \qquad \left(\frac{2M - n}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{n}{p}\right).$$

Wenn daher zunächst $p = 4z + 1$ ist, so sind die beiden Zahlen n, $2M - n$, falls n weder M noch $2M$ ist, gleichzeitig trigonale Reste oder gleichzeitig trigonale Nichtreste; da nun in diesem Falle aufser M nach Schlufs von 1) auch $2M$ ein trigonaler Rest ist, so werden sich die übrigen $\frac{p-5}{2}$ trigonalen Reste, ebenso die $\frac{p-1}{2}$ trigonalen Nichtreste in Paare zusammenfassen lassen, derart dafs die Summe eines jeden Paares $\equiv 2M \pmod{p}$ ist.

Wenn dagegen $p = 4z + 3$ ist, so ist der Gleichung (300) zufolge von den beiden Zahlen n, $2M - n$, falls n von M und $2M$ verschieden ist, die eine ein trigonaler Rest, die andere ein Nichtrest. Da nun in diesem Falle M ein trigonaler Rest, aber $2M$ ein trigonaler Nichtrest ist, so wird von den übrigen $\frac{p-3}{2}$ trigonalen Resten und den übrigen $\frac{p-3}{2}$ trigonalen Nichtresten immer ein Rest und ein Nichtrest zu einem Paare sich zusammenstellen lassen, derart dafs wieder die Summe eines jeden Paares $\equiv 2M \pmod{p}$ ist. Hierbei ist jedoch ersichtlich $p > 3$ anzunehmen, da sonst nur die beiden Zahlen M, $2M$ in betracht kommen.

4) Betrachtet man statt der Zahlen $\frac{x(x+1)}{2}$ die Zahlen $x(x+1)$, so sollen die von Null verschiedenen Reste derselben $(\text{mod. } p)$ — oder auch irgend welche, ihnen kongruente Zahlen — bitrigonale Reste von p genannt werden.

Aus dem für die trigonalen Reste Bewiesenen geht nun unmittelbar hervor, dafs es $\frac{p-1}{2}$ bitrigonale Reste und ebensoviel bitrigonale Nichtreste giebt, und dafs unter den ersteren der Rest des Mittelgliedes $\frac{p^2-1}{4}$ mit $2M \pmod{p}$ kongruent also gleich $\frac{p-1}{4}$ oder $\frac{3p-1}{4}$ ist, jenachdem p von der Form $4z + 1$ oder $4z + 3$ ist.

Fragt man, analog mit 2), nach den bitrigonalen Resten, die zugleich quadratische Reste sein können, so wird man auf die Frage geführt, wieviel Lösungen von der Form (298) die Kongruenz

$$X^2 - Y^2 \equiv 1 \pmod{p}$$

zuläfst; und eine ganz analoge Betrachtung wie dort läfst erkennen, dafs es für die Primzahlen $p=4z+1$ gleichviel quadratische Reste wie quadratische Nichtreste, für die Primzahlen $p=4z+3$ aber einen quadratischen Rest weniger als quadratische Nichtreste unter den bitrigonalen Resten giebt.

32. Diese Betrachtungen sind von Stern (*Journ. f. Math.* 71, 1870, p. 137) mit den Sätzen der Nr. 30 verbunden und so weitere Beziehungen zwischen den quadratischen und den trigonalen bezw. bitrigonalen Resten oder Nichtresten gewonnen worden, von denen wenigstens ein Teil hier noch Aufnahme finden soll.

Dabei bezeichnen wir wieder mit a, b die quadratischen, mit α, β die bitrigonalen, mit γ, δ die trigonalen Reste bezw. Nichtreste in der Reihe $1, 2, 3, \cdots p-1$; speziell sei a_x der kleinste positive Rest von x^2; α_x, γ_x diejenigen von $x(x+1)$, $\frac{x(x+1)}{2}$ resp. Dann folgt aus der Identität

$$(301) \qquad (x+1)^2 = \frac{x(x+1)}{2} + \frac{(x+1)(x+2)}{2}$$

die Kongruenz

$$a_{x+1} \equiv \gamma_x + \gamma_{x+1} \pmod{p}$$

und daher die Gleichung

$$a_{x+1} = \gamma_x + \gamma_{x+1} - l_x \cdot p,$$

unter l_x die Null oder die Eins verstanden, jenachdem die Summe $\gamma_x + \gamma_{x+1} < p$ oder $> p$ ist. Setzt man hier $x = 0, 1, 2, \cdots \frac{p-3}{2}$ und addiert die so hervorgehenden Gleichungen, so findet sich links die Summe aller quadratischen Reste a, rechts entsteht aus γ_{x+1} die Summe aller trigonalen Reste, aus γ_x dieselbe Summe bis auf das letzte Glied $\gamma_{\frac{p-1}{2}} = M$, und so erhält man die Beziehung

$$(302) \qquad \sum a = 2 \cdot \sum \gamma - M - l \cdot p,$$

in welcher l Null oder eine positive ganze Zahl $\overline{\gtrless} \frac{p-3}{2}$ ist. Man erkennt hieraus, dafs die Summe der quadratischen Reste (mod. p) stets kleiner ist, als die doppelte Summe der trigonalen Reste.

Da sowohl die quadratischen wie die trigonalen Reste und Nichtreste zusammengenommen alle Zahlen $1, 2, 3, \cdots p-1$ erschöpfen, so besteht die Gleichheit

$$\sum a + \sum b = \sum \gamma + \sum \delta;$$

aus $\sum a < 2 \sum \gamma$ folgt also

$$2\sum a - \left(\sum a + \sum b\right) < 4\sum \gamma - \left(\sum \gamma + \sum \delta\right)$$

d. i.

$$\sum a - \sum b < 3\sum \gamma - \sum \delta.$$

Da für Primzahlen $p = 4z + 1$ nach (276) die linke Seite dieser Ungleichheit verschwindet, zeigt sich, dafs für Primzahlen von der Form $4z+1$ die Summe der trigonalen Nichtreste kleiner ist als die dreifache Summe der trigonalen Reste.

Geht man statt von (301) von der gleichbedeutenden Identität

$$2(x+1)^2 = x(x+1) + (x+1)(x+2)$$

aus, verfährt in gleicher Weise wie vorher und nennt dabei c_x den kleinsten positiven Rest von $2x^2$, so entsteht die Gleichung

$$(303) \qquad c_{x+1} = \alpha_x + \alpha_{x+1} - l_x \cdot p,$$

worin wieder l_x gleich Null oder Eins ist, jenachdem die Summe $\alpha_x + \alpha_{x+1} < p$ oder $> p$ ist. Nun sind die Reste der Zahlen $2 \cdot 1^2$, $2 \cdot 2^2, \cdots 2 \cdot \left(\frac{p-1}{2}\right)^2$, jenachdem 2 quadratischer Rest oder Nichtrest von p ist, d. h. jenachdem p eine der Formen $8z + 1$, $8z + 7$ oder eine der Formen $8z + 3$, $8z + 5$ hat, die sämtlichen quadratischen Reste bezw. Nichtreste von p. Durch Addition der Gleichungen (303) für $x = 0, 1, 2, \cdots \frac{p-3}{2}$ ergiebt sich also je nach diesen beiden Fällen die erste oder die zweite der nachstehenden Beziehungen:

$$(304) \qquad \sum a = 2\sum \alpha - \alpha_{\frac{p-1}{2}} - l \cdot p$$

$$(305) \qquad \sum b = 2\sum \alpha - \alpha_{\frac{p-1}{2}} - l \cdot p,$$

worin wieder l Null oder eine positive ganze Zahl $\overline{\gtrless} \frac{p-3}{2}$ ist. Die zweite derselben läfst sich, wenn $p = 8z + 5$ ist, mit Rücksicht auf (276) durch die erste ersetzen. Ist dagegen $p = 8z + 3$, so ist nach (287)

$$\sum a < 2\sum \alpha - \alpha_{\frac{p-1}{2}} - l \cdot p,$$

und somit schliefst man für jede Primzahl p die Ungleichheit

$$\sum a < 2\sum \alpha$$

d. h. den Satz: die Summe der quadratischen Reste (mod. p) ist stets kleiner als die doppelte Summe der bitrigonalen Reste.

Der Unterschied zwischen den letztbezeichneten beiden Summen kann jedoch noch genauer bestimmt werden. Da man die bitrigonalen

Reste offenbar auch findet, indem man die kleinsten positiven Reste des Ausdrucks

$$\left(\frac{p-1}{2}-x\right)\left(\frac{p+1}{2}-x\right)=\frac{p^2-1}{4}-px+x^2$$

oder auch diejenigen des Ausdrucks

$$\frac{p^2-1}{4}+x^2$$

(mod. p) für $x=0,1,2,\cdots\frac{p-3}{2}$ bildet, so wird, wenn unter $\varrho(x)$ der kleinste positive Rest von x (mod. p) verstanden wird,

$$\sum\alpha=\sum_{x=0}^{\frac{p-3}{2}}\varrho\left(\frac{p^2-1}{4}+x^2\right)$$

oder auch, da $\frac{p^2-1}{4}+x^2$ für $x=\frac{p-1}{2}$ mit Null (mod. p) kongruent wird,

$$\sum\alpha=\sum_{x=0}^{\frac{p-1}{2}}\varrho\left(\frac{p^2-1}{4}+x^2\right) \tag{306}$$

sein. Desgleichen findet sich

$$\sum a=\sum_{x=0}^{\frac{p-1}{2}}\varrho(x^2). \tag{307}$$

Ist nun zuerst $p=4z+1$, so wird $\frac{p^2-1}{4}=4z^2+2z=pz+z$, also

$$\varrho\left(\frac{p^2-1}{4}+x^2\right)=\varrho(z+x^2);$$

daher ist für diejenigen x, denen quadratische Reste $<3z+1$ entsprechen,

$$\varrho\left(\frac{p^2-1}{4}+x^2\right)=z+\varrho(x^2),$$

für diejenigen x dagegen, denen quadratische Reste $\overline{\gtrless}\, 3z+1$ entsprechen,

$$\varrho\left(\frac{p^2-1}{4}+x^2\right)=z+\varrho(x^2)-p,$$

also findet man aus (306) und (307)

$$\sum\alpha=\sum a+\frac{p+1}{2}z-p\cdot\lambda,$$

wenn λ die Anzahl der quadratischen Reste bezeichnet, welche $\overline{\gtrless}\, 3z+1$ oder auch, was für Primzahlen der angenommenen Form ersichtlich dasselbe sagt, welche $\overline{\lessgtr}\, z<\frac{p}{4}$ sind; λ ist also dasselbe,

wie die in Nr. 30 mit A_1 bezeichnete Anzahl. Durch Multiplikation mit 2 nimmt die gewonnene Gleichung folgende Gestalt an:

$$(308) \qquad 2\sum \alpha = 2\sum a + z - p\,(2A_1 - z).$$

Ist aber zweitens $p = 4z + 3$, so wird $\frac{p^2-1}{4} = 4z^2 + 6z + 2 = pz + 3z + 2$, also

$$\varrho\left(\frac{p^2-1}{4} + x^2\right) = \varrho(3z + 2 + x^2);$$

mithin ist

$$\varrho\left(\frac{p^2-1}{4} + x^2\right) = 3z + 2 + \varrho(x^2)$$

für diejenigen x, denen quadratische Reste $\overline{\gtrless}\, z$ entsprechen, dagegen

$$\varrho\left(\frac{p^2-1}{4} + x^2\right) = 3z + 2 + \varrho(x^2) - p$$

für diejenigen x, denen quadratische Reste $> z$ d. i. $> \frac{p}{4}$ entsprechen. Hieraus ergiebt sich nach (306) und (307)

$$\sum \alpha = \sum a + (3z + 2)\frac{p+1}{2} - p \cdot \lambda,$$

wenn λ die Anzahl der quadratischen Reste $> \frac{p}{4}$ d. i. die Anzahl

$$A_2 + A_3 + A_4 = \frac{p-1}{2} - A_1$$

bedeutet. Durch Multiplikation mit 2 findet sich folglich aus der vorigen Gleichung die neue:

$$(309) \qquad 2\sum \alpha = 2\sum a + 3z + 2 + p\,(2A_1 - z).$$

Nach dem nun, was in Nr. 30 auf Grund der Dirichletschen Sätze über den Wert von $2A_1 - z$ bemerkt worden ist, lehren die Formeln (308), (309) den ferneren Satz: Die Summe der bitrigonalen Reste (mod. p) ist kleiner oder gröfser als die der quadratischen Reste, jenachdem p von der Form $4z + 1$ oder $4z + 3$ ist.

Insbesondere folgt aus (308) mit Rücksicht auf (276), dafs für $p = 4z + 1$:

$$(310) \qquad \sum \alpha = (3p + 1) \cdot \frac{p-1}{8} - pA_1$$

ist; desgleichen aus (309), wenn z gerade, also $p = 8z' + 3$ ist, in welchem Falle $2A_1 - z = 0$ war,

$$(311) \qquad \sum \alpha = \sum a + \frac{3p-1}{8};$$

ist dagegen z ungerade d. h. $p = 8z' + 7$, so bedarf es, um die Formel (309) auf ihre einfachste Gestalt zu bringen, noch des oben erwähnten Dirichletschen Satzes, nach welchem

$$A_1 + A_2 - B_1 - B_2 = \left(2 - \left(\frac{2}{p}\right)\right) \cdot \frac{\Sigma b - \Sigma a}{p}$$

d. h. im gegenwärtigen Falle wegen (284) und weil $A_1 + B_1$ die Anzahl aller Zahlen $< \frac{p}{4}$ also gleich z ist,

(312) $$2A_1 - z = \frac{\Sigma b - \Sigma a}{p}$$

ist; mit Hilfe hiervon und von (281) ergiebt sich dann

(313) $$\sum \alpha = \frac{3p-1}{8} + \frac{p(p-1)}{4}.$$

33. Da die bitrigonalen ebenso wie die quadratischen Reste und Nichtreste zusammengenommen die Reihe der Zahlen 1, 2, 3, $\cdots p-1$ erschöpfen, so ist

(314) $$\sum \alpha + \sum \beta = \sum a + \sum b = \frac{p(p-1)}{2}.$$

Falls $p = 4z + 1$ ist, nimmt diese Beziehung wegen (276) die Gestalt an:

$$\sum \alpha + \sum \beta = 2 \cdot \sum a;$$

da nun im gleichen Falle $\sum \alpha < \sum a$ gefunden worden, so ist umgekehrt $\sum \beta > \sum a$ und demnach auch

$$\sum \beta > \sum \alpha,$$

die Summe der bitrigonalen Nichtreste ist gröfser als die der Reste. Auch findet sich aus (310) und (314) die Differenz

$$\sum \beta - \sum \alpha = 2A_1 \cdot p - (p+1) \cdot \frac{p-1}{4}$$

ist also gerade.

Ist zweitens $p = 8z' + 3 > 3$, so folgt aus (311) und (314)

$$\sum \beta - \sum \alpha = \sum b - \sum a - \frac{3p-1}{4}.$$

Dem zuvor angezogenen Dirichletschen Satze zufolge ist aber $\sum b - \sum a = p\Delta$, wo Δ eine positive ganze Zahl und, weil auch $\sum a + \sum b = \frac{p(p-1)}{2}$ ein Vielfaches von p und ungerade ist, eine ungerade Zahl bedeutet. Hieraus folgt ersichtlich, dafs auch jetzt wieder die Summe der bitrigonalen Nichtreste die der Reste übertrifft, die Differenz $\sum \beta - \sum \alpha$ dagegen ungerade ist.

Wenn endlich $p = 8z' + 7$ ist, folgt aus (313) und (314) ohne weiteres

$$\sum \alpha - \sum \beta = \frac{3p-1}{4};$$

jetzt ist also die Summe der bitrigonalen Reste gröfser als die der Nichtreste, die Differenz beider aber wieder ungerade.

Um in dieser Hinsicht auch die Summe der trigonalen Reste und Nichtreste zu vergleichen, bemerke man, dafs aus

$$x(x+1) = p\xi + \alpha_x,$$

wo α_x der bitrigonale Rest also $< p$ ist, die Gleichungen

$$\frac{x(x+1)}{2} = p \cdot \frac{\xi}{2} + \frac{\alpha_x}{2}$$

$$\frac{x(x+1)}{2} = p \cdot \frac{\xi - 1}{2} + \frac{p + \alpha_x}{2}$$

d. h. die Beziehungen $\gamma_x = \frac{\alpha_x}{2}$ oder $\gamma_x = \frac{p + \alpha_x}{2}$ hervorgeht, jenachdem α_x gerade oder ungerade ist. Bezeichnet man also mit u die Anzahl der ungeraden bitrigonalen Reste, so ergiebt sich sofort die Gleichung:

$$\sum \gamma = \frac{1}{2} \sum \alpha + \frac{pu}{2}, \tag{315}$$

woraus in Verbindung mit der Gleichheit

$$\sum \gamma + \sum \delta = \sum \alpha + \sum \beta = \frac{p(p-1)}{2} \tag{316}$$

sich die andere:

$$\sum \delta - \sum \gamma = \sum \beta - pu \tag{317}$$

ergiebt. Die erste Beziehung lehrt, dafs u gleichzeitig mit $\sum \alpha$ gerade bezw. ungerade ist. Zufolge (316) sind aber, jenachdem p von der Form $4z + 1$ oder $4z + 3$ ist, $\sum \alpha, \sum \beta$ gleichartige resp. ungleichartige Zahlen. Im erstern Falle sind also u und $\sum \beta$ gleichartige, im zweiten ungleichartige Zahlen und demnach findet man: die Differenz

$$\sum \delta - \sum \gamma$$

ist gerade oder ungerade, jenachdem $p = 4z + 1$ oder $p = 4z + 3$ ist.

Nun hat Stern, worauf hier jedoch nicht weiter mehr eingegangen werden soll, wie für die quadratischen, so auch für die trigonalen und die bitrigonalen Reste und Nichtreste ihre Verteilung über die Intervalle $0, \frac{p}{4}; \frac{p}{4}, \frac{p}{2}; \frac{p}{2}, \frac{3p}{4}; \frac{3p}{4}, p$ näher untersucht. Neben anderen Resultaten, die er hierbei erzielt hat und von denen nur die beiden erwähnt seien, dafs, wenn p von der Form $8z + 3$ oder $8z + 5$ ist, $\sum b < 2 \sum a$ resp. $< 3 \sum a$ ist, hat er gefunden,

dafs die Anzahl u der ungeraden bitrigonalen Reste immer kleiner als $\frac{p}{4}$ ist, und auf Grund dieser Thatsache den weiteren Satz:

$$\sum\delta - \sum\gamma > 0,$$

d. h. dafs die Summe der trigonalen Nichtreste gröfser als die der Reste ist. Indem wir für die Herleitung desselben den Leser auf Sterns Arbeit selbst verweisen, wollen wir zum Abschlusse dieser Betrachtungen noch einen andern Satz ausführlich begründen, welcher die Anzahl der bitrigonalen und der quadratischen Reste in gewissen Intervallen in Beziehung zu einander setzt.

Aus dem in Nr. 31 unter 1) und 3) für die trigonalen Reste Bewiesenen geht hervor, dafs, wenn $p = 4z + 1$ ist, die kleinsten positiven Reste $\frac{p-1}{4}, \frac{p-1}{2}$ der Zahlen $2M$, $4M$ (mod. p) bitrigonale Reste sind. Sieht man von diesen beiden bitrigonalen Resten ab, so lassen sich die übrigen paarweise so zusammenstellen, dafs die Summe eines jeden Paares kongruent mit $4M$ d. i. mit $\frac{p-1}{2}$ wird; hieraus leuchtet ein, dafs von den Gliedern eines Paares nicht das eine $< \frac{p}{2}$, das andere $> \frac{p}{2}$ sein kann, und dafs für jedes Paar von solchen Resten, die $< \frac{p}{2}$ sind, die Summe gleich $\frac{p-1}{2}$, dagegen für jedes Paar von solchen, welche $> \frac{p}{2}$ sind, die Summe gleich $p + \frac{p-1}{2}$ sein wird. Heifst mithin r die Anzahl der bitrigonalen Reste, die $< \frac{p}{2}$ sind, zu welchen die beiden vorher abgesonderten Reste $\frac{p-1}{4}, \frac{p-1}{2}$ zu rechnen sind, so erhält man nachstehende Gleichheit:

$$\sum\alpha = \frac{p-1}{4} + \frac{p-1}{2} + \frac{r-2}{2} \cdot \frac{p-1}{2} + \frac{\frac{p-1}{2} - r}{2} \cdot \left(p + \frac{p-1}{2}\right)$$

oder, vereinfacht:

$$\sum\alpha = (3p+1) \cdot \frac{p-1}{8} - p \cdot \frac{r}{2},$$

eine Formel, deren Vergleichung mit (310)

$$r = 2A_1$$

ergiebt. Für die Anzahl der bitrigonalen Nichtreste, welche $< \frac{p}{2}$ sind, ergiebt sich hieraus der Wert

$$\frac{p-1}{2} - r = \frac{p-1}{2} - 2A_1$$

d. i. wegen $A_1 + B_1 = \frac{p-1}{4}$ der Wert $2B_1$. Man hat demnach den

Satz: Ist $p = 4z + 1$, so ist die Anzahl der bitrigonalen Reste (Nichtreste) zwischen 0 und $\frac{p}{2}$ doppelt so grofs, als die der quadratischen Reste (Nichtreste) zwischen 0 und $\frac{p}{4}$. —

Siebentes Kapitel.

Die höheren Kongruenzen.

1. Nachdem im Vorigen die Theorie der quadratischen Kongruenzen ausführlich behandelt worden, soll nunmehr diejenige der Kongruenzen höheren Grades, soweit sie der niederen Zahlentheorie zugerechnet werden kann, ihre Erledigung finden. Wie man aber in der Lehre von den Gleichungen die Betrachtung der allgemeinen Gleichungen m^{ten} Grades auf diejenige der sogenannten reinen oder binomischen Gleichungen zurückführt, so werden wir auch hier mit der Untersuchung der binomischen Kongruenzen d. i. der Kongruenzen von der Form

$$x^m \equiv a \pmod{n} \tag{1}$$

beginnen. Wir setzen dabei a als relativ prim zu n voraus.

Ist diese Kongruenz auflösbar, giebt es also eine ganze Zahl x, deren m^{te} Potenz mit $a \pmod{n}$ kongruent ist, so heifst a ein m^{ter} Potenzrest, im entgegengesetzten Falle ein m^{ter} Nichtrest (mod. n).

Angenommen nun, a sei ein m^{ter} Potenzrest (mod. n) und $x \equiv \xi$ (mod. n) eine Wurzel der Kongruenz (1); ξ ist dann prim gegen n. Ist z irgend eine Lösung der Kongruenz

$$z^m \equiv 1 \pmod{n}, \tag{2}$$

wie es eine solche, nämlich die Lösung $z = 1$, gewifs stets giebt, so folgt aus der Verbindung dieser Kongruenz mit der anderen:

$$\xi^m \equiv a \pmod{n}$$

die dritte:

$$(\xi z)^m \equiv a \pmod{n},$$

man erhält mithin aus einer Lösung ξ von (1) durch Multiplikation mit jeder Lösung z von (2) wieder eine Lösung $\xi' = \xi z$ von (1). Ist umgekehrt ξ' eine von ξ verschiedene Lösung von (1) und ξ_1 der Socius von ξ, so folgt aus den Kongruenzen

$$\xi'^m \equiv \xi^m, \quad \xi\xi_1 \equiv 1 \pmod{n}$$

sogleich die andere:

$$(\xi'\xi_1)^m \equiv 1 \pmod{n},$$

mithin ist $\xi'\xi_1$ eine Lösung z von (2) und folglich $\xi' \equiv \xi z \pmod{n}$; jede Lösung von (1) entsteht also aus einer derselben durch Multiplikation mit einer Lösung von (2). Hiernach sind die Lösungen der Kongruenz (1) identisch mit den Zahlen ξ', welche die Formel

$$\xi' \equiv \xi z \pmod{n} \tag{3}$$

ergiebt, wenn darin für ξ **eine** Lösung von (1), für z **jede** Lösung von (2) eingesetzt wird.

Es handelt sich daher vor allem darum, die sämtlichen Lösungen der Kongruenz (2) zu ermitteln.

Gesetzt nun, z leiste gleichzeitig zwei Kongruenzen von der Gestalt (2), etwa den Kongruenzen

$$z^r \equiv 1, \quad z^s \equiv 1 \pmod{n} \tag{4}$$

Genüge, so wird jedenfalls z prim gegen n sein, also einen Socius z_1 besitzen; aus den vorstehenden Kongruenzen ergiebt sich dann

$$(zz_1)^s \equiv z_1^s \quad \text{d. h.} \quad z_1^s \equiv 1 \pmod{n}$$

und nun für beliebige positive ganze Werte x, y die Kongruenz

$$z^{rx} \cdot z_1^{sy} \equiv 1 \pmod{n},$$

der man die folgende Gestalt:

$$z^{rx-sy} \cdot (zz_1)^{sy} \equiv 1 \pmod{n}$$

geben kann. Wählt man also die ganzen Zahlen x, y so, dafs

$$rx - sy = d$$

d. i. gleich dem gröfsten gemeinsamen Teiler von r, s wird, so ergiebt sich

$$z^d \equiv 1 \pmod{n}. \tag{5}$$

Genügt also eine Zahl z den beiden Kongruenzen (4), so genügt sie auch der Kongruenz (5), deren Grad der gröfste gemeinsame Teiler der Grade der ersteren ist.

Hiernach genügt jede Wurzel der Kongruenz (2), weil sie prim ist gegen n also dem allgemeinen Fermatschen Satze zufolge zugleich der Kongruenz

$$z^{\varphi(n)} \equiv 1 \pmod{n} \tag{6}$$

genügen mufs, auch der Kongruenz

$$z^d \equiv 1 \pmod{n}, \tag{7}$$

deren Grad d der gröfste gemeinsame Teiler von m und $\varphi(n)$ ist. Da aber auch umgekehrt aus (7)

$$z^m \equiv (z^d)^{\frac{m}{d}} \equiv 1 \pmod{n}$$

hervorgeht, jede Wurzel von (7) folglich auch eine solche von (2) ist, so erkennt man, daſs die Wurzeln der Kongruenz (2) völlig identisch sind mit den Wurzeln der Kongruenz (7). Der Grad der letzteren ist ein Teiler von $\varphi(n)$; um alle Kongruenzen von der Gestalt (2) zu lösen, darf man sich daher auf diejenigen beschränken, deren Grad ein Divisor von $\varphi(n)$ ist. Wir setzen also in der Folge den Grad der Kongruenz (2) stets als einen Teiler von $\varphi(n)$ voraus.

Wäre m kein Teiler von $\varphi(n)$, so würde der gröſste gemeinsame Teiler d von m und $\varphi(n)$ kleiner als m, die Kongruenz (7) also von geringerem Grade sein, als die Kongruenz (2). Bedeutet daher

$$z^\delta \equiv 1 \pmod{n}$$

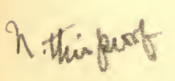
die Kongruenz geringsten Grades von der Gestalt (2), der eine Zahl z Genüge thut, so muſs notwendig δ ein Teiler von $\varphi(n)$ sein. Wir werden dann sagen: die Zahl z gehöre (mod. n) zum Exponenten δ. Da jede zu n prime Zahl z einer Kongruenz von der Gestalt (2), jedenfalls nämlich der Kongruenz (6), und folglich auch einer solchen Kongruenz niedrigsten Grades genügen muſs, so ergiebt sich hieraus der Satz: Jede zu n prime Zahl gehört (mod. n) zu einem bestimmten Exponenten, der immer ein Teiler von $\varphi(n)$ ist.

Was wir so gefunden haben, indem wir uns auf den allgemeinen Fermatschen Satz stützten, läſst sich auch unmittelbar herleiten und giebt dann umgekehrt einen neuen Beweis dieses Satzes. In der That, ist z eine zu n prime Zahl, so werden auch die sämtlichen Potenzen $1, z, z^2, z^3, \dots$ prim gegen n sein; da es nun nur $\varphi(n)$ inkongruente Zahlen ohne gemeinsamen Teiler mit n giebt, so können jene unendlich vielen Potenzen nicht sämtlich inkongruent sein; sind also etwa z^h und z^{h+m} kongruent, so ergiebt sich $z^m \equiv 1 \pmod{n}$, folglich giebt es für jede zu n prime Zahl z eine Potenz, welche (mod. n) der Einheit kongruent ist. Unter allen solchen giebt es mithin auch eine niedrigste Potenz $z^\delta \equiv 1 \pmod{n}$ d. h. z gehört zu einem gewissen Exponenten δ (mod. n).

Dann sind aber die δ Potenzen

$$1, z, z^2, \dots z^{\delta-1} \tag{8}$$

sämtlich inkongruent, weil aus der Kongruenz $z^k \equiv z^{i+k}$ zweier von ihnen sich $z^i \equiv 1 \pmod{n}$ ergäbe, während $i < \delta$ wäre, gegen die Bedeutung des Exponenten δ. Entweder ist nun $\delta = \varphi(n)$ oder $< \varphi(n)$. Im letztern Falle giebt es noch eine Zahl α, welche keiner der δ Potenzen (8) kongruent ist; alsdann werden die δ Zahlen



$$\alpha, \alpha z, \alpha z^2, \dots \alpha z^{\delta-1} \tag{9}$$

sowohl unter einander, als auch mit den Zahlen (8) inkongruent sein, denn aus $\alpha z^k \equiv \alpha z^{i+k}$ folgte wieder $z^i \equiv 1$, während $i < \delta$ ist, aus $\alpha z^k \equiv z^h$ aber folgte $\alpha z^\delta \equiv z^{\delta+h-k}$ d. i. $\alpha \equiv z^i$, wo i der kleinste positive Rest von $\delta + h - k$ (mod. δ) ist, α wäre also gegen die Voraussetzung einer der Zahlen (8) kongruent. Entweder ist nun $2\delta = \varphi(n)$ d. h. die Zahlen (8) und (9) erfüllen das ganze reduzierte Restsystem (mod. n), oder es ist $2\delta < \varphi(n)$. In diesem Falle sei β eine Zahl, welche keiner der Zahlen (8) oder (9) kongruent ist; alsdann sind die Zahlen

$$(10) \qquad \beta,\ \beta z,\ \beta z^2,\ \ldots\ \beta z^{\delta-1}$$

wieder sowohl unter sich als mit den Zahlen (8) inkongruent; sie sind es aber weiter auch mit den Zahlen (9), denn aus $\beta z^k \equiv \alpha z^h$ würde $\beta \equiv \alpha z^i$ d. h. kongruent mit einer der Zahlen (9) befunden, gegen die Voraussetzung. Ist nun auch 3δ noch kleiner als $\varphi(n)$, so läfst sich sogleich wieder eine neue Reihe von δ Zahlen angeben, welche zu n prim sind, u. s. w. Da aber endlich die Menge dieser Zahlen erschöpft werden mufs, so findet sich notwendig

$$\alpha\delta = \varphi(n)$$

d. h. δ als ein Teiler von $\varphi(n)$. Der Exponent also, zu welchem eine zu n prime Zahl (mod. n) gehört, ist immer ein Teiler von $\varphi(n)$.

Da aus $z^\delta \equiv 1$ (mod. n) für jedes Vielfache $h\delta$ von δ auch $z^{h\delta} \equiv 1$ (mod. n) hervorgeht, so findet sich dem letzten Satze zufolge insbesondere auch

$$(11) \qquad z^{\varphi(n)} \equiv 1 \pmod{n}$$

d. h. ein neuer Beweis des verallgemeinerten Fermatschen Satzes. (S. denselben für den Fall $n = p$ bei Gaufs *D. A. art.* 50).

Gehört die Zahl z zum Exponenten δ (mod. n), so sind, wie gezeigt, die Potenzen (8) inkongruent, jede andere Potenz von z aber ist einer von ihnen kongruent (mod. n). Denn, setzt man $m = h\delta + r$, wo $0 \overline{\gtrless} r < \delta$, so ergiebt sich

$$z^m = z^{h\delta} \cdot z^r \equiv z^r \pmod{n},$$

wo z^r eine der Potenzen (8). Ebenso ist $z^{m'} \equiv z^{r'}$ (mod. n), wenn $m' = h'\delta + r'$, $0 \overline{\gtrless} r' < \delta$ gesetzt wird. Da nun z^r, $z^{r'}$ dann und nur dann kongruent sind (mod. n), wenn sie eine und dieselbe der Potenzen (8) vorstellen d. h. wenn $r = r'$ ist, so werden zwei Potenzen z^m, $z^{m'}$ dann und nur dann (mod. n) kongruent sein, wenn $m \equiv m'$ (mod. δ) ist. Insbesondere wird die Kongruenz

$$(12) \qquad z^m \equiv 1 \pmod{n}$$

dann und nur dann erfüllt sein, wenn $m \equiv 0$ (mod. δ), wenn nämlich m ein Vielfaches von δ ist.

Die Reihe der Potenzen (8) wird die Periode der Zahl z genannt.

2. Wenn der Exponent δ, zu welchem eine zu n prime Zahl z gehört, der, wie gezeigt, stets aufgeht in $\varphi(n)$, gleich $\varphi(n)$ ist, so wird die Zahl z eine primitive Wurzel (mod. n) genannt. In diesem Falle wäre $z^{\varphi(n)}$ die niedrigste Potenz, welche der Einheit kongruent wird (mod. n). Da nun nach Kap. 5, Nr. 3 für jede Zahl z, welche prim ist gegen

$$n = p^\alpha q^\beta r^\gamma \ldots, \tag{13}$$

bereits

$$z^{\psi(n)} \equiv 1 \pmod{n}$$

ist, wo $\psi(n)$ das kleinste gemeinsame Vielfache der Zahlen $\varphi(p^\alpha)$, $\varphi(q^\beta)$, $\varphi(r^\gamma) \ldots$ bedeutet, deren Produkt gleich $\varphi(n)$ ist, so kann für den Modulus n nur dann eine primitive Wurzel existieren, wenn $\psi(n) = \varphi(n)$, das kleinste gemeinsame Vielfache jener Zahlen ihrem Produkte gleich ist, d. h. wenn jene Zahlen zu je zweien relativ prim sind. Hiernach giebt es (mod. n) keine primitive Wurzel, wenn in der Zerlegung (13) mindestens zwei ungerade Primfaktoren p, q vorhanden sind, denn

$$\varphi(p^\alpha) = p^{\alpha-1} \cdot (p-1), \quad \varphi(q^\beta) = q^{\beta-1} \cdot (q-1)$$

haben stets den gemeinsamen Teiler 2. Man müfste also

$$n = 2^\lambda \cdot p^\alpha$$

voraussetzen. Ist hier aber $\alpha > 0$, der ungerade Primfaktor p also wirklich vorhanden, so darf λ nicht > 1 sein, denn sonst hätten

$$\varphi(2^\lambda) = 2^{\lambda-1}, \quad \varphi(p^\alpha) = p^{\alpha-1} \cdot (p-1)$$

wieder den gemeinsamen Teiler 2. Man erschliefst also das Resultat: eine primitive Wurzel (mod. n) giebt es möglicherweise nur in den folgenden drei Fällen:

$$n = 2^\lambda, \quad n = p^\alpha, \quad n = 2p^\alpha.$$

Ob in diesen Fällen aber wirklich solche Wurzeln existieren, bleibt noch zu entscheiden.

Wir betrachten zu diesem Zwecke zunächst den Fall $n = p$, und stellen in ihm uns die allgemeinere Frage: giebt es Zahlen, welche zu einem beliebig gegebenen Teiler δ von $\varphi(p) = p - 1$ als Exponenten (mod. p) gehören?

Offenbar wären die inkongruenten Zahlen dieser Art identisch mit den primitiven d. h. denjenigen Wurzeln der Kongruenz

$$z^\delta \equiv 1 \pmod{p}, \tag{14}$$

welche keiner Kongruenz von derselben Gestalt aber von niedrigerem Grade genügen. Die Anzahl dieser Wurzeln nennen

wir für einen Augenblick $\chi(\delta)$; entweder ist sie Null, wenn keine derartige Wurzel, oder, wie leicht zu zeigen, gleich $\varphi(\delta)$, sobald eine solche vorhanden ist. Ist nämlich ζ eine solche Wurzel also eine zum Exponenten δ (mod. p) gehörige Zahl, so ist jede der Potenzen $1, \zeta, \zeta^2, \zeta^3, \ldots$, von denen die ersten δ:

$$(15) \qquad 1, \zeta, \zeta^2, \ldots \zeta^{\delta-1}$$

inkongruent sind, jedenfalls auch eine Wurzel der Kongruenz (14), und da die letztere nicht mehr Wurzeln haben kann, als ihr Grad beträgt (Kap. 3 Nr. 4), so hat sie deren genau δ und die Periode (15) stellt diese sämtlichen Wurzeln dar. Bezeichnet aber d für eine dieser Wurzeln, ζ^h, den gröfsten gemeinsamen Teiler von h und δ, sodafs, wenn $h = h'd$, $\delta = \delta'd$ gesetzt wird, h', δ' relativ prim sind, so wird dann und nur dann

$$(\zeta^h)^m = \zeta^{h'dm} \equiv 1 \pmod{p}$$

sein, wenn $h'dm$ ein Vielfaches von $\delta'd$ d. h. $h'm$ ein solches von δ' also m durch δ' teilbar, $m = k\delta'$ ist; der kleinste dieser Werte ist $m = \delta'$, demnach gehört ζ^h (mod. p) zum Exponenten $\delta' = \frac{\delta}{d}$ und daher dann und nur dann zum Exponenten δ, wenn $d = 1$ d. h. wenn h und δ relativ prim sind. Von den durch die Potenzen (15) dargestellten Wurzeln der Kongruenz (14) sind mithin $\varphi(\delta)$ primitiv, wie behauptet.

Man beachte nun, dafs jede nicht primitive Wurzel der Kongruenz (14), da sie zu einem gewissen Exponenten δ' (mod. p) gehört, primitive Wurzel einer Kongruenz

$$(16) \qquad z^{\delta'} \equiv 1 \pmod{p}$$

sein mufs, deren Grad δ' ein Teiler von δ ist, letzteres, da auch $z^\delta \equiv 1$ (mod. p) sein soll. Umgekehrt wird aber auch, wenn δ' ein Teiler von δ ist, jede, also auch jede primitive Wurzel von (16) der Kongruenz (14) genügen. Hieraus folgt offenbar: dafs man die sämtlichen Wurzeln der Kongruenz (14) erhält, wenn man für alle diejenigen Kongruenzen (16), deren Grade den sämtlichen Teilern von δ, diese Zahl selbst mit einbegriffen, gleich sind, die primitiven Wurzeln aufstellt.

Die Kongruenz (14) hat aber δ Wurzeln. Denn, da δ als ein Teiler von $p-1$ vorausgesetzt ist, sodafs $p-1 = d\delta$ gesetzt werden kann, so ist

$$z^{p-1} - 1 = (z^\delta - 1)\,(z^{\delta(d-1)} + z^{\delta(d-2)} + \cdots + z^\delta + 1);$$

da nun nach dem Fermatschen Satze die linke Seite dieser Gleichung für jede der $p-1$ Zahlen $1, 2, 3, \cdots p-1$ durch p teilbar wird, so wird dies auch für jeden dieser Werte einer der beiden Faktoren zur Rechten, und da eine Kongruenz (mod. p) nicht für mehr dieser

Zahlen erfüllt sein kann, als ihr Grad beträgt, so mufs jeder der genannten Faktoren genau für soviel derselben durch p teilbar werden, als sein Grad beträgt, der Faktor $z^\delta - 1$ also für δ derselben, w. z. b. w.

Aus der Verbindung dieses Resultats mit dem voraufgehenden folgt sogleich die Beziehung

$$\delta = \chi(1) + \chi(\delta') + \chi(\delta'') + \cdots + \chi(\delta),$$

wo $1, \delta', \delta'', \cdots \delta$ die sämtlichen Teiler von δ bedeuten. Bekanntlich ist aber auch

$$\delta = \varphi(1) + \varphi(\delta') + \varphi(\delta'') + \cdots + \varphi(\delta)$$

und daher

$$\chi(1) + \chi(\delta') + \cdots + \chi(\delta) = \varphi(1) + \varphi(\delta') + \cdots + \varphi(\delta).$$

Nun ist bereits gezeigt, dafs jedes Glied der linken Seite Null oder dem entsprechenden Gliede der rechten Seite gleich ist; wäre daher auch nur ein einziges Mal ein Glied der linken Seite wirklich Null, so könnte die Gleichheit beider Seiten nicht bestehen und somit mufs jedes Glied der einen dem entsprechenden Gliede der anderen Seite gleich sein, insbesondere also auch

$$\chi(\delta) = \varphi(\delta). \tag{17}$$

Auf solche Weise ist festgestellt: dafs es für jeden Teiler δ von $p-1$ Zahlen giebt, welche (mod. p) zum Exponenten δ gehören; ihre Anzahl beträgt $\varphi(\delta)$.

Setzt man $\delta = p - 1$ voraus, so ergiebt sich insbesondere der Satz: es giebt $\varphi(p-1)$ inkongruente primitive Wurzeln (mod. p).

3. Dies überaus wichtige Resultat soll durch eine zweite Herleitung bestätigt werden. Sei

$$p - 1 = a^\alpha b^\beta c^\gamma \ldots,$$

wo $a, b, c, \ldots$ die verschiedenen Primfaktoren bedeuten, aus denen sich $p-1$ zusammensetzt. Man überzeugt sich zunächst leicht, dafs die Kongruenz

$$z^{a^\alpha} \equiv 1 \pmod{p} \tag{18}$$

primitive Wurzeln besitzt; in der That hat sie nach dem bezüglich der Kongruenz (14) Bewiesenen a^α Wurzeln, und jede nicht primitive Wurzel derselben müfste einer Kongruenz derselben Gestalt genügen, deren Grad ein von a^α verschiedener Teiler von a^α d. h. eine niedrigere Potenz von a wäre und also aufginge in $a^{\alpha-1}$; sie genügte jedenfalls also auch der Kongruenz

$$z^{a^{\alpha-1}} \equiv 1 \pmod{p}, \tag{19}$$

wie denn auch umgekehrt jede Wurzel der letzteren eine nicht primitive Wurzel von (18) ist. Die Anzahl der nicht primitiven Wurzeln

der Kongruenz (18) ist demnach gleich der Anzahl der Wurzeln der Kongruenz (19) d. i. gleich $a^{\alpha-1}$; folglich hat die Kongruenz (18) primitive Wurzeln und ihre Anzahl beträgt

$$a^{\alpha} - a^{\alpha-1} = \varphi(a^{\alpha}).$$

Ebenso hat die Kongruenz

$$z^{b^{\beta}} \equiv 1 \pmod{p}$$

$\varphi(b^{\beta})$, die Kongruenz

$$z^{c^{\gamma}} \equiv 1 \pmod{p}$$

$\varphi(c^{\gamma})$ primitive Wurzeln, u. s. w.

Nun bedeute $\zeta, \eta, \theta, \cdots$ jede Wurzel der Kongruenz

$$(20) \qquad z^{a^{\alpha}} \equiv 1, \quad z^{b^{\beta}} \equiv 1, \quad z^{c^{\gamma}} \equiv 1, \cdots \pmod{p}$$

resp.; dann liefert der Ausdruck

$$(21) \qquad \zeta\eta\theta\cdots$$

sämtliche Wurzeln der Kongruenz

$$(22) \qquad z^{a^{\alpha} b^{\beta} c^{\gamma} \cdots} \equiv 1 \pmod{p},$$

und zwar die primitiven oder die nicht primitiven derselben, jenachdem $\zeta, \eta, \theta, \cdots$ sämtlich oder nicht sämtlich primitive Wurzeln der bezüglichen Kongruenzen sind. In der That ist

$$\begin{array}{llll}
\text{wegen } \zeta^{a^{\alpha}} \equiv 1 & \text{auch} & \zeta^{a^{\alpha} b^{\beta} c^{\gamma} \cdots} \equiv 1 & \pmod{p} \\
\;\;\text{„} \quad \eta^{b^{\beta}} \equiv 1 & \text{„} & \eta^{a^{\alpha} b^{\beta} c^{\gamma} \cdots} \equiv 1 & \text{„} \\
\;\;\text{„} \quad \theta^{c^{\gamma}} \equiv 1 & \text{„} & \theta^{a^{\alpha} b^{\beta} c^{\gamma} \cdots} \equiv 1 & \text{„} \\
\cdots & \cdots & \cdots & \cdots
\end{array}$$

und folglich auch

$$(\zeta\eta\theta\cdots)^{a^{\alpha} b^{\beta} c^{\gamma} \cdots} \equiv 1 \pmod{p}$$

d. h. $\zeta\eta\theta\cdots$ ist eine Wurzel der Kongruenz (22). Die den verschiedenen Wurzelkombinationen $\zeta, \eta, \theta, \cdots$ entsprechenden Ausdrücke $\zeta\eta\theta\cdots$ aber, deren Anzahl

$$a^{\alpha} b^{\beta} c^{\gamma} \cdots = p - 1$$

ist, sind unter einander inkongruent. Denn, wären zwei von ihnen kongruent:

$$\zeta\eta\theta\cdots \equiv \zeta'\eta'\theta'\cdots \pmod{p}$$

so fände sich durch Erhebung in die $b^{\beta} c^{\gamma} \cdots{}^{\text{te}}$ Potenz

$$\zeta^{b^{\beta} c^{\gamma} \cdots} \equiv \zeta'^{\, b^{\beta} c^{\gamma} \cdots} \pmod{p};$$

da auch

$$\zeta^{a^{\alpha}} \equiv \zeta'^{\, a^{\alpha}} \pmod{p}$$

ist, so fände sich durch eine Betrachtung, analog der bei den Kongruenzen (4) angewendeten, auch

$$\zeta^d \equiv \zeta'^d \pmod{p},$$

wo d den gröfsten gemeinsamen Teiler der Exponenten $a^\alpha, b^\beta \cdot c^\gamma \ldots$, d. h. die Einheit bedeutet. Also fände sich $\zeta = \zeta'$; ganz ebenso aber auch $\eta = \eta'$, $\theta = \theta', \ldots$ gegen die Voraussetzung. Da nun für die Kongruenz (22) die Anzahl der Wurzeln ebenfalls $p-1$ beträgt, so liefert der Ausdruck (21), wie zunächst behauptet, diese sämtlichen Wurzeln. — Ist jetzt wenigstens eine der Wurzeln $\zeta, \eta, \theta, \ldots$, z. B. ζ, eine nicht primitive Wurzel der entsprechenden der Kongruenzen (20), so würde schon $\zeta^{a^{\alpha-1}} \equiv 1$ und daher

$$(\zeta\eta\theta\cdots)^{a^{\alpha-1}b^\beta c^\gamma\cdots} \equiv \zeta^{a^{\alpha-1}b^\beta c^\gamma\cdots} \equiv 1 \pmod{p},$$

$\zeta\eta\theta\ldots$ also, wie ferner behauptet, eine nicht primitive Wurzel der Kongruenz (22) sein. Sind dagegen $\zeta, \eta, \theta, \ldots$ sämtlich primitive Wurzeln der bezüglichen Kongruenzen, so mufs auch $\zeta\eta\theta\ldots$ eine primitive Wurzel von (22) sein. Zum Beweise hiervon stützen wir uns auf den folgenden, an sich beachtenswerten

Hilfssatz: Gehören z', z'' (mod. p) zu den Exponenten d', d'', welche relativ prim sind, so gehört $z'z''$ (mod. p) zum Exponenten $d'd''$. Denn, nennt man s den Exponenten, zu welchem $z'z''$ gehört, so mufs

$$(z'z'')^{d's} \equiv z''^{d's} \equiv 1$$

$$(z'z'')^{d''s} \equiv z'^{d''s} \equiv 1$$

und folglich der ersten Kongruenz wegen $d's$ also auch s durch d'', der zweiten wegen $d''s$ also auch s durch d' und somit s durch $d'd''$ teilbar sein; jedoch ist bereits

$$(z'z'')^{d'd''} \equiv (z'^{d'})^{d''} \cdot (z''^{d''})^{d'} \equiv 1 \pmod{p},$$

also auch umgekehrt $d'd''$ teilbar durch s und somit $s = d'd''$, w. z. b. w.

Diesem Hilfssatze gemäfs gehört zunächst, falls ζ, η primitive Wurzeln der beiden ersten Kongruenzen (20) also Zahlen sind, die zu den relativ primen Exponenten a^α, b^β gehören, $\zeta\eta$ zum Exponenten $a^\alpha \cdot b^\beta$; desgleichen gehört, wenn auch θ eine primitive Wurzel der dritten jener Kongruenzen ist, $\zeta\eta\theta$ zum Exponenten $a^\alpha b^\beta c^\gamma$ u. s. w., endlich $\zeta\eta\theta\ldots$ zum Exponenten $a^\alpha b^\beta c^\gamma \ldots$, ist also eine primitive Wurzel (mod. p).

Hiermit ist der ausgesprochene Satz in allen Stücken bewiesen.

Verbindet man ihn aber mit dem für die einfachere Kongruenz (18) zuvor Bewiesenen, so ergiebt sich nicht nur die Existenz

primitiver Wurzeln der Kongruenz (22) d. h. primitiver Wurzeln (mod. p), sondern auch deren Anzahl:

$$\varphi(a^\alpha)\cdot\varphi(b^\beta)\cdot\varphi(c^\gamma)\cdots=\varphi(p-1)=\varphi(\varphi(p)).$$

4. Indem wir uns nun zu dem allgemeineren Falle $n=p^\alpha$ wenden, beginnen wir die Untersuchung, ob es auch in ihm primitive Wurzeln (mod. n) giebt, mit dem Beweise eines Hilfssatzes. Dabei soll gesagt werden, z^m-1 sei genau durch p^h teilbar, wenn es zwar durch p^h, nicht aber durch p^{h+1} aufgeht. Der gemeinte Satz lautet dann folgendermafsen:

Ist z^m-1 genau durch p^h teilbar $(h>0)$, so ist es $z^{pm}-1$ genau durch p^{h+1}, und umgekehrt.

Ist nämlich $z^m-1=p^h\cdot k$, so folgt aus dem binomischen Lehrsatze:

$$z^{pm}-1=p\cdot p^hk+\frac{p(p-1)}{2}\cdot p^{2h}k^2+\cdots$$
$$=p^{h+1}\left(k+\frac{p(p-1)}{2}\cdot p^{h-1}k^2+\cdots\right)=p^{h+1}\cdot k'$$

wo k', wenn k nicht mehr durch p teilbar ist, auch nicht durch p mehr aufgeht, was die erste Behauptung ist. Ist aber umgekehrt $z^{pm}-1$ genau durch p^{h+1} teilbar, so mufs es z^m-1 genau durch p^h sein; denn wäre z^m-1 genau durch $p^{h'}$ teilbar, so würde $h'>0$ und dem soeben Bewiesenen zufolge $z^{pm}-1$ genau durch $p^{h'+1}$ teilbar sein, und es ergiebt sich also $h'=h$.

Dies vorausgeschickt, bemerke man, dafs, wenn z eine primitive Wurzel von p^α, also $z^{p^{\alpha-1}(p-1)}$ die niedrigste Potenz von z sein soll, welche (mod. p^α) der Einheit kongruent ist, z notwendig auch primitive Wurzel (mod. p) sein mufs. Denn, wäre schon $z^m-1\equiv 0$ (mod. p), wo $m<p-1$, so würde dem Beweise des Hilfssatzes zufolge $z^{pm}-1\equiv 0$ (mod. p^2), $z^{p^2m}-1\equiv 0$ (mod. p^3), ... also gewifs schon

$$z^{p^{\alpha-1}\cdot m}\equiv 1 \pmod{p^\alpha}$$

mithin z nicht primitive Wurzel (mod. p^α) sein.

Sei daher jetzt g irgend eine primitive Wurzel (mod. p) und δ der Exponent, zu welchem sie (mod. p^α) gehört. Der letztere ist, wie bekannt, ein Teiler von $p^{\alpha-1}(p-1)$. Da aber aus

$$g^\delta\equiv 1 \pmod{p^\alpha} \tag{23}$$

auch $g^\delta\equiv 1$ (mod. p) folgt und g primitive Wurzel (mod. p) ist, so mufs andererseits δ ein Vielfaches von $p-1$ sein. Demnach ist

$$\delta=p^{\alpha-\lambda}\cdot(p-1),$$

wo λ eine der Zahlen $1, 2, 3, \ldots \alpha$ sein kann. Zur näheren Bestimmung von λ nenne man p^h die höchste in $g^{p-1}-1$ aufgehende

Potenz von p; dann ist nach dem Hilfssatze $g^{p^{\alpha-\lambda}(p-1)}-1$ genau teilbar durch $p^{\alpha+h-\lambda}$ und es ergiebt sich wegen (23) $h \gtreqless \lambda$; wäre aber $h > \lambda$, so wäre demselben Hilfssatze zufolge schon $g^{p^{\alpha-h}\cdot(p-1)}-1$ teilbar durch p^α, gegen die Bedeutung des Exponenten δ. Man findet also $h=\lambda$ und somit den Satz:

Ist g eine primitive Wurzel (mod. p) und p^λ die höchste Potenz von p, welche in $g^{p-1}-1$ aufgeht, so ist der Exponent, zu welchem g (mod. p^α) gehört,

$$\delta = p^{\alpha-\lambda}\cdot(p-1). \tag{24}$$

Hieraus folgt sogleich weiter: Die primitive Wurzel g (mod. p) ist dann und nur dann zugleich eine primitive Wurzel (mod. p^α), wenn die durch p teilbare Differenz $g^{p-1}-1$ nicht teilbar ist durch p^2; denn in diesem und nur in diesem Falle ist $\lambda=1$, also der Exponent, zu welchem g (mod. p^α) gehört,

$$\delta = p^{\alpha-1}\cdot(p-1).$$

Nun giebt es aber stets primitive Wurzeln g (mod. p), für welche $g^{p-1}-1$ nicht teilbar durch p^2 ist. Wäre nämlich $g^{p-1}-1=kp^2$, so setze man

$$\gamma = g + zp;$$

aus dieser Gleichung oder aus der Kongruenz $\gamma\equiv g$ (mod. p) folgt für jeden ganzzahligen Exponenten h

$$\gamma^h \equiv g^h \pmod{p},$$

mithin wird, welche ganze Zahl auch für z gewählt werde, γ mit g zugleich primitive Wurzel (mod. p) sein; da aber

$$\begin{aligned}\gamma^{p-1}-1 &= g^{p-1}-1+\frac{p-1}{1}g^{p-2}zp+\frac{(p-1)(p-2)}{1\cdot 2}g^{p-3}z^2p^2+\cdots\\ &= p\left(kp+\frac{p-1}{1}g^{p-2}z+\frac{(p-1)(p-2)}{1\cdot 2}g^{p-3}z^2p+\cdots\right)\end{aligned}$$

gefunden wird, so kann offenbar $\gamma^{p-1}-1$ durch p^2 nicht teilbar sein, wenn z als nicht durch p teilbar gewählt wird.

Die Verbindung dieses Resultats mit dem voraufgehenden führt zu dem Satze: Es giebt stets primitive Wurzeln (mod. p^α), und man findet sie sämtlich, wenn man diejenigen primitiven Wurzeln g (mod. p) bestimmt, für welche $g^{p-1}-1$ nicht teilbar ist durch p^2.

Leicht erkennt man nunmehr, dafs auch (mod. $2p^\alpha$) primitive Wurzeln vorhanden sind. In der That, sei γ eine primitive Wurzel (mod. p^α); mit γ zugleich ist es auch die kongruente Zahl $\gamma+p^\alpha$, eine dieser beiden Zahlen aber ist ungerade, sie heifse g.

Diese Zahl g ist eine primitive Wurzel (mod. $2p^\alpha$) d. h. zum Exponenten $\varphi(2p^\alpha) = p^{\alpha-1} \cdot (p-1)$ gehörig; denn erstens ist wegen

$$g \equiv 1 \pmod{2}, \quad g \equiv \gamma \pmod{p^\alpha}$$

für jeden der Moduln $2, p^\alpha$, folglich auch für den Modulus $2p^\alpha$

$$g^{p^{\alpha-1}\cdot(p-1)} \equiv 1;$$

wäre aber bereits $g^m \equiv 1$ (mod. $2p^\alpha$), wo $m < p^{\alpha-1}(p-1)$, so würde, gegen die Bedeutung der Zahl g, diese Kongruenz auch (mod. p^α) erfüllt sein.

Behalten wir hier diese Bedeutung bei, so bilden die Potenzen

$$g, g^2, g^3, \cdots g^{p^{\alpha-1}(p-1)} \tag{25}$$

ein reduziertes Restsystem für jeden der beiden Moduln p^α, $2p^\alpha$, jede zu p^α resp. $2p^\alpha$ prime Zahl z ist also einer bestimmten dieser Potenzen kongruent. Denn erstens ist die Anzahl dieser Potenzen gleich der Anzahl

$$\varphi(p^\alpha) = p^{\alpha-1} \cdot (p-1) = \varphi(2p^\alpha) \tag{26}$$

der Glieder eines solchen Restsystems; zweitens aber sind jene Potenzen auch unter einander inkongruente, zu p^α resp. $2p^\alpha$ prime Zahlen, denn aus der Kongruenz zweier derselben:

$$g^h \equiv g^{h+k},$$

wo $0 < h,\ h + k \overline{\gtrless} p^{\alpha-1}(p-1)$ gedacht ist, ergäbe sich die Kongruenz $g^k \equiv 1$, während $k < p^{\alpha-1}(p-1)$ wäre, gegen die Bedeutung von g.

Untersuchen wir nun für eine beliebige der Potenzen (25) den Exponenten δ, zu welchem sie (mod. p^α bezw. $2p^\alpha$) gehört. Da dieser Exponent bekanntlich ein Teiler von $\varphi(p^\alpha)$ ist, sei δ irgend ein solcher Teiler, also

$$\varphi(p^\alpha) = d\delta.$$

Nun ist $(g^h)^\delta \equiv 1$ d. h. g^h dann und nur dann eine Wurzel der Kongruenz

$$z^\delta \equiv 1 \text{ (mod. } p^\alpha \text{ bezw. } 2p^\alpha), \tag{27}$$

wenn

$$h\delta = k \cdot \varphi(p^\alpha), \tag{28}$$

nämlich $h\delta$ ein Vielfaches von $\varphi(p^\alpha)$ ist, oder wenn $h = kd$ d. i. h ein Vielfaches von d ist. Da solcher Vielfachen in der Reihe der Exponenten $1, 2, 3, \ldots \varphi(p^\alpha)$ genau δ vorhanden sind, so folgt zunächst: Die Kongruenz (27) hat genau δ Wurzeln.

Ferner aber ist $z \equiv g^h$ eine primitive Wurzel von (27) dann und nur dann, wenn δ die kleinste Zahl ist, für welche eine Gleichung von der Gestalt (28) stattfindet d. h. wenn $h\delta$ das kleinste gemein-

same Vielfache von h und $\varphi(p^\alpha) = d\delta$ ist; letzteres ist $\frac{h \cdot d\delta}{t}$, wenn t gröfster gemeinsamer Teiler von h und $d\delta$ ist; es müfste also $t = d$ sein. Somit gehört g^h zum Exponenten $\delta = \frac{\varphi(p^\alpha)}{d}$ dann und nur dann, wenn d gröfster gemeinsamer Teiler von h und $\varphi(p^\alpha)$ ist.

Daher giebt es so viel der Potenzen (25) oder, da diese ein reduziertes Restsystem (mod. p^α bezw. $2p^\alpha$) bilden, so viel inkongruente Glieder eines solchen Restsystems, welche zum Exponenten δ gehören, als es in der Reihe der Exponenten $1, 2, 3, \ldots p^{\alpha-1}(p-1)$ Zahlen giebt, die mit $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ den gröfsten gemeinsamen Teiler d besitzen, d. h. $\varphi\left(\frac{\varphi(p^\alpha)}{d}\right) = \varphi(\delta)$.

Insbesondere giebt es $\varphi(\varphi(p^\alpha))$ zum Exponenten $\varphi(p^\alpha)$ gehörige Potenzen (25) d. h. inkongruente primitive Wurzeln (mod. p^α bezw. $2p^\alpha$).

Aus der Herleitung dieser Sätze geht hervor, dafs eine Zahl $z \equiv g^h$ dann zum Exponenten $\delta = \frac{\varphi(p^\alpha)}{d}$ gehört, wenn $h = kd$ und k prim ist gegen δ. Bezeichnet nun c gleichfalls eine zu δ prime Zahl, so ist auch ck eine solche, und somit $z^c \equiv g^{ckd}$ wieder eine zum Exponenten δ gehörige Zahl. Wenn daher $1, c', c'', \ldots$ ein reduziertes Restsystem (mod. δ) bilden, so sind $z, z^{c'}, z^{c''}, \ldots \varphi(\delta)$ zum Exponenten δ gehörige und zwar inkongruente Zahlen, denn aus $z^{c'} \equiv z^{c''}$ oder $g^{c'h} \equiv g^{c''h}$ folgte $g^{(c'-c'')h} \equiv 1$ d. h. $(c'-c'')kd$ teilbar durch $\varphi(p^\alpha) = \delta d$ oder $(c'-c'')k$ durch δ, was nicht sein kann, da k prim zu δ und c', c'' (mod. δ) inkongruent sind. Da nun nur $\varphi(\delta)$ inkongruente, zum Exponenten δ gehörige Zahlen vorhanden sind, so ergiebt sich der Satz: Ist z irgend eine der zum Exponenten δ gehörigen Zahlen d. i. irgend **eine primitive Wurzel** der Kongruenz (27), so stellen die Potenzen

$$(29) \qquad z, z^{c'}, z^{c''}, \ldots,$$

in denen $1, c', c'', \ldots$ irgend ein reduziertes Restsystem (mod. δ) bezeichnen, die sämtlichen **primitiven Wurzeln** derselben d. h. alle inkongruenten, zum Exponenten δ gehörigen Zahlen dar. Die **sämtlichen** Wurzeln der Kongruenz (27) sind die Potenzen

$$(30) \qquad 1, z, z^2, \ldots z^{\delta-1},$$

denn diese ergeben sich wieder als inkongruent und genügen jener Kongruenz mit z zugleich.

5. Es erübrigt endlich der Fall $n = 2^\lambda$.

Nun darf zunächst für $\lambda = 1$ d. h. für den Modulus $n = 2$ die Zahl 1 als primitive Wurzel angesehen werden.

Für $\lambda = 2$ d. h. für den Modulus $n = 4$ ist -1 primitive Wurzel, da erst $(-1)^2 \equiv 1 \pmod{4}$ ist.

Für den Modulus $n = 2^\lambda$ aber, wo $\lambda > 2$ ist, giebt es keine primitiven Wurzeln mehr, vielmehr ist hier bereits die $2^{\lambda-2}$te Potenz jeder zu 2^λ primen d. i. ungeraden Zahl z kongruent 1:

$$z^{2^{\lambda-2}} \equiv 1 \pmod{2^\lambda}. \tag{31}$$

In der That trifft dies zu für $\lambda = 3$ d. h. für $n = 8$, da bereits das Quadrat jeder ungeraden Zahl den Rest 1 läfst. Ist es nun auch richtig für den Modulus 2^λ, also

$$z^{2^{\lambda-2}} = 1 + 2^\lambda \cdot k,$$

so ergiebt sich

$$z^{2^{\lambda-1}} = (1 + 2^\lambda k)^2 = 1 + 2^{\lambda+1}(k + 2^{\lambda-1}k^2),$$

es ist also auch noch richtig für den Modulus $2^{\lambda+1}$ und gilt somit allgemein.

Man beachte, dafs die Kongruenz (31) zum Unterschiede von denjenigen, deren Modulus eine Primzahl ist, mehr Wurzeln hat, als ihr Grad beträgt, nämlich die $2^{\lambda-1}$ ungeraden Zahlen $< 2^\lambda$.

Giebt es nun auch, wie gezeigt, in diesem Falle keine primitiven Wurzeln für den Modulus 2^λ, so giebt es doch primitive Wurzeln der Kongruenz (31) oder Zahlen, welche zum Exponenten $2^{\lambda-2}$ gehören. Eine solche Zahl ist $z = 5$. In der That müfste offenbar sonst 5 zu einem Exponenten gehören, der ein Teiler von $2^{\lambda-2}$ wäre, müfste jedenfalls also

$$5^{2^{\lambda-3}} \equiv 1 \pmod{2^\lambda}$$

sein, während doch, wie leicht einzusehen,

$$5^{2^{\lambda-3}} \equiv 1 + 2^{\lambda-1} \pmod{2^\lambda}$$

ist. Dies leuchtet ohne weiteres ein für $\lambda = 3$; nehmen wir aber an, es sei auch schon für einen Wert $\lambda \geqq 3$ bewiesen, so folgern wir sogleich

$$5^{2^{\lambda-2}} \equiv 1 + 2^\lambda \pmod{2^{\lambda+1}}$$

also die Richtigkeit der Aussage noch für den nächstgröfseren Wert von λ und somit ihre Allgemeingiltigkeit.

Hieraus schliefst man leicht, dafs die Potenzen

$$\left\{\begin{array}{l} 1, \quad 5, \quad 5^2, \quad 5^3, \cdots \quad 5^{2^{\lambda-2}-1}, \\ -1, \ -5, \ -5^2, \ -5^3, \cdots \ -5^{2^{\lambda-2}-1} \end{array}\right. \tag{32}$$

ein reduziertes Restsystem (mod. 2^λ) ausmachen. In der That sind zwei Potenzen der ersten sowohl wie der zweiten Reihe in-

kongruente ungerade Zahlen, da aus $\pm 5^h \equiv \pm 5^{h+i}$, wo $h, i, h+i < 2^{\lambda-2}$, sich sogleich $5^i \equiv 1$ ergäbe, gegen das bereits Bewiesene; aber auch die Potenzen der einen Reihe sind inkongruent zu denen der anderen, denn, wären sie kongruent (mod. 2^λ), so müfsten sie es auch sein (mod. 4), die der ersteren Reihe aber sind von der Form $4k+1$, die der anderen von der Form $4k+3$; in (32) hat man also $2 \cdot 2^{\lambda-2} = 2^{\lambda-1}$ (mod. 2^λ) inkongruente ungerade Zahlen, w. z. b. w. Jede ungerade Zahl ist mithin einer der Potenzen (32) (mod. 2^λ) kongruent.

Es fragt sich, zu welchem Exponenten δ eine dieser Potenzen gehört.

Zunächst leuchtet ein, dafs der fragliche Exponent nur ein Teiler von $2^{\lambda-2}$ also nur eine der Potenzen

$$(33) \qquad 1,\ 2,\ 2^2,\ \ldots\ 2^{\lambda-3},\ 2^{\lambda-2}$$

sein kann; ferner, dafs die Zahl 1 zum Exponenten 1, die Zahl -1 zum Exponenten 2 gehört. Sei jetzt 5^k eine Potenz, deren Exponent k von Null verschieden ist, und $k = 2^\mu u$, wo u ungerade; μ ist einer der Werte $0, 1, 2, \cdots \lambda - 3$. Soll dann

$$(34) \qquad 5^{k\delta} = 5^{u \cdot 2^\mu \delta} \equiv 1 \text{ (mod. } 2^\lambda)$$

sein, so mufs $u \cdot 2^\mu \delta$ durch $2^{\lambda-2}$ also δ durch $2^{\lambda-\mu-2}$ teilbar sein, und da schon $\delta = 2^{\lambda-\mu-2}$ der Kongruenz (34) genügt, so gehört 5^k zum Exponenten $2^{\lambda-\mu-2}$. Zu demselben Exponenten gehört aber auch -5^k; denn, soll $(-5^k)^\delta \equiv 1$ (mod. 2^λ) sein, so mufs $5^{k\delta} \equiv \pm 1$ oder vielmehr, da wegen $\lambda > 2$ das untere Vorzeichen unmöglich ist, da sonst auch $5^{k\delta} \equiv -1$ (mod. 4) sein müfste, es mufs $5^{k\delta} \equiv +1$ (mod. 2^λ) also $\delta = 2^{\lambda-\mu-2}$ sein, und umgekehrt folgt auch hieraus wieder $(-5^k)^\delta \equiv 1$, da $\delta = 2^{\lambda-\mu-2}$ gerade ist. Demnach gehören zum Exponenten $\delta = 2^{\lambda-\mu-2}$ doppelt soviel Potenzen (32), als es in der Reihe $1, 2, 3, \cdots 2^{\lambda-2} - 1$ Zahlen giebt, welche ungerade Vielfache von 2^μ sind, mithin $2 \cdot 2^{\lambda-\mu-3} = 2^{\lambda-\mu-2}$ Potenzen, ausgenommen den Fall $\mu = \lambda - 3$ d. i. $\delta = 2$, in welchem aufser den Potenzen $5^{2^{\lambda-3}}$, $-5^{2^{\lambda-3}}$ noch die zuvor betrachtete Zahl -1, also drei Zahlen der Reihen (32) zum Exponenten 2 gehören. Man schliefst also den Satz:

Zu den Exponenten (33) gehören (mod. 2^λ) resp.

$$1,\ 3,\ 2^2,\ \cdots\ 2^{\lambda-3},\ 2^{\lambda-2}$$

inkongruente ungerade Zahlen.

Beachtet man ferner, dafs die Wurzeln der Kongruenz

$$(35) \qquad z^{2^h} \equiv 1 \text{ (mod. } 2^\lambda), \quad 0 < h \overline{\gtrless} \lambda - 2$$

mit den primitiven Wurzeln der Kongruenzen

$$z \equiv 1, \quad z^2 \equiv 1, \quad z^{2^2} \equiv 1, \cdots z^{2^{h-1}} \equiv 1, \quad z^{2^h} \equiv 1$$

d. h. mit den zu den Exponenten $1, 2, 2^2, \ldots 2^h$ gehörigen inkongruenten ungeraden Zahlen übereinstimmen müssen, so ergiebt sich als Gesamtanzahl der Wurzeln der Kongruenz (35) die Zahl

$$1 + 3 + 2^2 + \cdots + 2^h = (1 + 2 + \cdots + 2^h) + 1 = 2^{h+1};$$

für $h = \lambda - 2$ erhält man hieraus die Gesamtanzahl der Wurzeln der Kongruenz (31) d. h. der inkongruenten ungeraden Zahlen (mod. 2^λ) gleich $2^{\lambda-1}$, wie es sein mufs.

6. Aus den in den letzten beiden Nummern erhaltenen Resultaten fliefst eine ganze Reihe wichtiger Folgerungen, zunächst aus Nr. 4 zwei Sätze von C. F. Arndt (s. *Journ. f. Math.* 31, 1846, p. 326), deren einfachste Fälle schon von Gaufs bewiesen worden sind.

1) Das **Produkt** aller inkongruenten, zu demselben Exponenten δ (mod. p^α bezw. $2p^\alpha$) gehörigen Zahlen ist kongruent 1, aufser wenn $\delta = 2$ ist. In der That, wir fanden, dafs, wenn z eine solche Zahl bezeichnet, sie sämtlich gegeben werden durch die Potenzen

$$z, z^{c'}, z^{c''}, \ldots, \tag{36}$$

in denen $1, c', c'', \ldots$ irgend ein reduziertes Restsystem (mod. δ) bedeuten. Ist nun $\delta > 2$, so ist mit c auch $\delta - c$ relativ prim zu δ, aber (mod. δ) von c verschieden, je zwei der $\varphi(\delta)$ Zahlen $1, c', c'', \ldots$ geben also eine durch δ teilbare Summe, sodafs auch

$$1 + c' + c'' + \cdots \equiv 0 \text{ (mod. } \delta)$$

folglich

$$z^{1+c'+c''+\cdots} \equiv 1 \text{ (mod. } p^\alpha \text{ bezw. } 2p^\alpha)$$

ist; dasselbe gilt für $\delta = 1$, denn die einzige zu diesem Exponenten gehörige Zahl ist Eins. Zum Exponenten $\delta = 2$ dagegen gehört nur die einzige Zahl -1.

Insbesondere ist hiernach das Produkt aller inkongruenten primitiven Wurzeln (mod. p^α bezw. $2p^\alpha$) kongruent 1, aufser, wenn $p^{\alpha-1}(p-1) = 2$, d. h. wenn der Modulus $p = 3$ ist. Dieser Satz findet sich für den Primzahlmodulus p schon bei Gaufs *D. A. art.* 80.

2) Die **Summe** aller inkongruenten, zu demselben Exponenten δ (mod. p^α bezw. $2p^\alpha$) gehörigen Zahlen ist kongruent 0, wenn δ einen Primfaktor mehrfach enthält, dagegen kongruent ± 1, wenn δ aus lauter ungleichen Primfaktoren besteht und zwar kongruent $+1$ oder -1, jenachdem die Anzahl der letzteren gerade oder ungerade ist.

Hat δ zuerst einen Primfaktor q mehrfach, sodafs $\frac{\delta}{q}$ durch q aufgeht, so besteht $\frac{\delta}{q}$ aus denselben Primfaktoren wie δ, und deshalb

ist mit c zugleich auch $c + h \cdot \frac{\delta}{q}$ prim gegen δ, welchen ganzzahligen Wert man für h auch setze. Daher zerfällt das reduzierte Restsystem (mod. δ) in eine Anzahl Reihen von je q Zahlen von der Form:

$$(37)\qquad \begin{array}{l} c,\ c+\frac{\delta}{q},\ c+2\frac{\delta}{q}, \cdots c+(q-1)\frac{\delta}{q}, \\ c_1,\ c_1+\frac{\delta}{q},\ c_1+2\frac{\delta}{q}, \cdots c_1+(q-1)\frac{\delta}{q}, \\ c_2,\ c_2+\frac{\delta}{q},\ c_2+2\frac{\delta}{q}, \cdots c_2+(q-1)\frac{\delta}{q}, \\ \cdots\cdots\cdots\cdots\cdots\cdots \end{array}$$

wo $c, c_1, c_2, \ldots$ zu δ prim und (mod. δ) inkongruent sind. Denn die Zahlen der ersten Reihe sind prim gegen δ und (mod. δ) inkongruent; erschöpft diese Reihe noch nicht das ganze reduzierte Restsystem (mod. δ), so giebt es eine mit keiner ihrer Zahlen kongruente gegen δ prime Zahl c_1, und somit liefert die zweite der Reihen (37) lauter, nicht nur unter sich, sondern offenbar auch mit denjenigen der ersten Reihe (mod. δ) inkongruente, zu δ prime Zahlen, u. s. w.; in der That ist in dem betrachteten Falle $\varphi(\delta)$ teilbar durch q, die Anzahl der sämtlichen Glieder des reduzierten Restsystems ein Vielfaches von q.

Sei nun z irgend eine zum Exponenten δ gehörige Zahl, so erhält man sie sämtlich, wenn man in z^k den Exponenten k die sämtlichen Zahlen (37) durchlaufen läſst. Da aber für jeden Index i d. h. für jede einzelne der Reihen (37) die Summe der ihr entsprechenden Glieder, nämlich

$$z^{c_i} + z^{c_i+\frac{\delta}{q}} + z^{c_i+2\frac{\delta}{q}} + \cdots + z^{c_i+(q-1)\frac{\delta}{q}}$$
$$= z^{c_i} \cdot \frac{z^{\delta}-1}{z^{\frac{\delta}{q}}-1} \equiv 0 \ (\text{mod. } p^{\alpha} \text{ bezw. } 2p^{\alpha})$$

gefunden wird, so muſs, wie behauptet, auch die Gesamtsumme aller zum Exponenten δ gehörigen Zahlen mit Null kongruent sein.

Ist dagegen zweitens $\delta = q_1 q_2 \ldots q_r$ aus r verschiedenen Primfaktoren zusammengesetzt, so giebt, wie sich aus der Formel (31) des 3. Kap. leicht erschlieſst, die Formel

$$k \equiv x_1\delta_1 + x_2\delta_2 + \cdots + x_r\delta_r \ (\text{mod. } \delta),$$

in welcher $\delta_i = \frac{\delta}{q_i}$ gedacht ist, alle inkongruenten, zu δ primen Zahlen k, wenn man allgemein x_i die Reihe der Zahlen $1, 2, 3, \cdots q_i-1$ durchlaufen läſst.

Daher ist die Summe

$$\sum z^k \equiv \sum z^{x_1\delta_1 + x_2\delta_2 + \cdots + x_r\delta_r} \pmod{p^\alpha \text{ bezw. } 2p^\alpha},$$

in welcher z irgend eine zum Exponenten δ gehörige Zahl bezeichnet, offenbar nichts anderes, als das entwickelte Produkt

$$\prod_i (z^{\delta_i} + z^{2\delta_i} + \cdots + z^{(q_i - 1)\delta_i}) = \prod_i \left(\frac{z^\delta - 1}{z^{\delta_i} - 1} - 1\right);$$

da aber $\frac{z^\delta - 1}{z^{\delta_i} - 1} \equiv 0$, der allgemeine Faktor des Produkts also $\equiv -1 \pmod{p^\alpha \text{ bezw. } 2p^\alpha}$ gefunden wird, so geht die Kongruenz

$$\sum z^k \equiv (-1)^r \pmod{p^\alpha \text{ bezw. } 2p^\alpha}$$

hervor, durch welche die auf den jetzt betrachteten Fall bezügliche Aussage des Satzes bestätigt wird.

Dem so bewiesenen zweiten Satze gemäfs ist insbesondere die Summe aller inkongruenten primitiven Wurzeln (mod. p^α bezw. $2p^\alpha$) d. i. aller zum Exponenten

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1) = \varphi(2p^\alpha)$$

gehörigen Zahlen gewifs kongruent Null, wenn $\alpha > 2$; andernfalls ist sie kongruent 0 oder ± 1, jenachdem $p - 1$ einen Primfaktor mehrfach enthält oder aus lauter verschiedenen Primfaktoren zusammengesetzt ist. Für den einfachsten Fall eines Primzahlmodulus gab diesen Satz schon Gaufs, *D. A. art.* 81. Setzt man nämlich, wie in Nr. 3,

$$p - 1 = a^\alpha b^\beta c^\gamma \ldots$$

und bezeichnet mit $\zeta, \eta, \theta, \ldots$ jede primitive Wurzel der Kongruenzen

$$z^{a^\alpha} \equiv 1, \quad z^{b^\beta} \equiv 1, \quad z^{c^\gamma} \equiv 1, \ldots \pmod{p} \tag{38}$$

resp., so giebt, wie dort gezeigt, der Ausdruck $\zeta\eta\theta\ldots$ sämtliche primitive Wurzeln (mod. p), und demnach ist die Summe der letzteren nichts anderes, als das entwickelte Produkt

$$(\zeta' + \zeta'' + \cdots)(\eta' + \eta'' + \cdots)(\theta' + \theta'' + \cdots)\cdots, \tag{39}$$

wo in den einzelnen Klammern die Summe der primitiven Wurzeln der entsprechenden Kongruenz (38) gedacht ist. Nun ist, wenn ζ eine primitive Wurzel der ersten dieser Kongruenzen bedeutet,

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{a^\alpha - 1} = \frac{\zeta^{a^\alpha} - 1}{\zeta - 1}$$

die Summe ihrer sämtlichen,

$$1 + \zeta^a + \zeta^{2a} + \cdots + \zeta^{(a^{\alpha-1} - 1)a} = \frac{\zeta^{a^\alpha} - 1}{\zeta^a - 1}$$

die Summen ihrer nicht primitiven Wurzeln; die erstere ist immer, die zweite für $\alpha > 1$ kongruent Null, für $\alpha = 1$ dagegen gleich 1. Daher wird der Unterschied beider Summen d. i. die Summe der primitiven Wurzeln der Kongruenz:

$$\zeta' + \zeta'' + \cdots \equiv 0 \text{ oder } \equiv -1 \pmod{p}$$

sein, jenachdem $\alpha > 1$ oder $\alpha = 1$ ist. Sobald also wenigstens einer der Exponenten $\alpha, \beta, \gamma, \cdots$ gröſser als 1, d. h. sobald $p-1$ einen Primfaktor mehrfach enthält, wird das Produkt (39) kongruent 0, andernfalls, wenn r die Anzahl der verschiedenen in $p-1$ enthaltenen Primfaktoren ist, kongruent $(-1)^r$ sein, w. z. b. w.

7. Hieran schlieſst sich ein neuer Beweis für den verallgemeinerten Wilsonschen Lehrsatz.*)

1) Sei zuerst der Modulus $n = p^\alpha$ oder $2p^\alpha$ und g irgend eine der primitiven Wurzeln desselben; dann bilden nach Nr. 4 die Potenzen (25):

$$g,\ g^2,\ g^3, \cdots g^{p^{\alpha-1}(p-1)}$$

ein reduziertes Restsystem für den Modulus n. Setzt man zur Abkürzung

$$p^{\alpha-1}(p-1) = \pi,$$

eine Zahl, welche stets gerade ist, so ergiebt sich das Produkt aller Glieder eines reduzierten Restsystems kongruent mit

$$g^{1+2+3+\ldots+\pi} = g^{\frac{\pi(\pi+1)}{2}} \tag{40}$$

Nun ist

$$g^\pi - 1 = (g^{\frac{\pi}{2}} - 1)(g^{\frac{\pi}{2}} + 1) \equiv 0 \pmod{p^\alpha \text{ bezw. } 2p^\alpha}.$$

Die beiden Faktoren, deren Differenz 2 ist, können nicht gleichzeitig durch p teilbar sein, daher muſs einer derselben durch p^α aufgehen, und dieser wird, falls der Modulus $2p^\alpha$ ist, in welchem Falle g ungerade ist, auch gerade sein d. i. aufgehen durch $2p^\alpha$. Da aber g primitive Wurzel des Modulus ist, kann nicht $g^{\frac{\pi}{2}} - 1 \equiv 0$ sein und folglich ist $g^{\frac{\pi}{2}} + 1 \equiv 0$ d. i. $g^{\frac{\pi}{2}} \equiv -1$. Hieraus folgt der Ausdruck (40) kongruent $(-1)^{\pi+1}$ oder, da π gerade ist, kongruent $-1 \pmod{p^\alpha \text{ bezw. } 2p^\alpha}$.

Man gelangt zu diesem Ergebnisse auch durch die Bemerkung, daſs die Glieder des reduzierten Restsystems sich in Gruppen verteilen, deren Elemente je zu ein- und demselben Teiler von π als Exponenten gehören, und daſs nach Nr. 6, 1) das Produkt der Zahlen

---

*) Den einfachen Wilsonschen Satz leitete schon Gauſs *D. A. art.* 76 in entsprechender Weise ab.

jeder einzelnen Gruppe kongruent 1 ist, mit Ausnahme derjenigen Gruppe, die zum Exponenten 2 gehört, welche nur aus der einen Zahl -1 besteht; das Produkt aller Glieder des reduzierten Restsystems ist mithin in der That kongruent -1.

2) Für den Modulus $n = 2$ besteht das reduzierte Restsystem aus der einzigen Zahl 1, zugleich aber ist $1 \equiv -1 \pmod{2}$.

3) Für den Modulus $n = 4$ bilden die Zahlen 1, 3 ein reduziertes Restsystem und man findet

$$1 \cdot 3 \equiv -1 \pmod{4}.$$

4) Ist aber $n = 2^\lambda$, $\lambda > 2$, so bilden die Potenzen (32) ein reduziertes Restsystem und folglich ist das Produkt aller Glieder eines solchen kongruent

$$(-1)^{2^{\lambda-2}} \cdot \left(5^{2^{\lambda-2}}\right)^{2^{\lambda-2}-1}$$

d. h. wegen $5^{2^{\lambda-2}} \equiv 1$ gleichfalls kongruent 1 $\pmod{2^\lambda}$.

Aus diesen besonderen Resultaten folgt aber der allgemeine Wilsonsche Satz durch eine Betrachtung analog derjenigen, die zum Beweise eines Satzes von Schemmel in Kap. 5 Nr. 10 verwandt worden ist. Sei

$$n = 2^\lambda p'^{\alpha'} p''^{\alpha''} \cdots; \tag{41}$$

dann giebt bekanntlich die Formel

$$\varrho \equiv \alpha r + \beta s + \gamma t + \cdots \pmod{n}$$

alle inkongruenten zu n primen Zahlen, wenn $r, s, t, \ldots$ die bekannten Hilfszahlen sind und $\alpha, \beta, \gamma, \ldots$ reduzierte Restsysteme resp. nach den Moduln $2^\lambda, p'^{\alpha'}, p''^{\alpha''}, \ldots$ durchlaufen. Die Anzahl der inkongruenten ϱ ist

$$\varphi(n) = \varphi(2^\lambda)\ \varphi(p'^{\alpha'})\ \varphi(p''^{\alpha''}) \cdots;$$

man setze

$$\varphi(2^\lambda) = \varphi,\ \varphi(p'^{\alpha'}) = \varphi',\ \varphi(p''^{\alpha''}) = \varphi'', \ldots$$

Da nun

$$\varrho \equiv \alpha \pmod{2^\lambda},\ \varrho \equiv \beta \pmod{p'^{\alpha'}},\ \varrho \equiv \gamma \pmod{p''^{\alpha''}}, \ldots$$

ist, so findet sich das über alle Glieder ϱ des reduzierten Restsystems $\pmod{n}$ erstreckte Produkt

$$\prod(\varrho) \equiv \prod(\alpha)^{\varphi'\varphi''\cdots} \pmod{2^\lambda}$$
$$\prod(\varrho) \equiv \prod(\beta)^{\varphi\varphi''\cdots} \pmod{p'^{\alpha'}}$$
$$\prod(\varrho) \equiv \prod(\gamma)^{\varphi\varphi'\cdots} \pmod{p''^{\alpha''}}$$
$$\cdots\cdots\cdots\cdots\cdots$$

Hier ist aber $\Pi(\alpha)$ und folglich auch $\Pi(\varrho)$ kongruent 1 $\pmod{2^\lambda}$ — nach 4) — wenn $\lambda > 2$; andernfalls ist zwar $\Pi(\alpha) \equiv -1$, gleich-

wohl wieder $\Pi(\varrho) \equiv +1$, wenn auch nur ein ungerader Primfaktor in n vorhanden ist, denn $\varphi', \varphi'', \ldots$ sind gerade Zahlen. Ferner ist zwar — nach 1) — $\Pi(\beta) \equiv -1 \pmod{p'^{\alpha'}}$, gleichwohl aber $\Pi(\varrho) \equiv +1$, wenn $\varphi\varphi'' \ldots$ gerade d. h. wenn noch ein zweiter ungerader Primfaktor in n aufgeht oder wenn $\lambda \gtreqless 2$ ist. Analog verhält es sich mit Bezug auf $(\text{mod.}\, p''^{\alpha''})$ u. s. w. Demnach ergiebt sich

$$\prod(\varrho) \equiv 1 \pmod{n},$$

wenn in (41) mehr als ein ungerader Primfaktor auftritt, oder wenn zwar nur ein solcher vorhanden, zugleich aber $\lambda \gtreqless 2$ ist, oder endlich, wenn kein ungerader Primfaktor vorhanden und zugleich $\lambda > 2$ ist. In allen übrigen Fällen, d. h. in den Fällen

$$n = 2,\ n = 4,\ n = p^\alpha,\ n = 2p^\alpha,$$

von welchen der erste auch dem vorigen zugerechnet werden darf, findet sich

$$\prod(\varrho) \equiv -1 \pmod{n}.$$

Dies ist aber genau, was der allgemeine Wilsonsche Satz behauptet.

8. Da die Potenzen (25) einer primitiven Wurzel g (mod. p^α bezw. $2p^\alpha$) ein reduziertes Restsystem bilden, mufs, wie schon bemerkt, jede zu p^α resp. $2p^\alpha$ prime Zahl z einer bestimmten dieser Potenzen kongruent:

$$z \equiv g^\gamma \ (\text{mod.}\, p^\alpha \text{ bezw. } 2p^\alpha) \tag{42}$$

sein; der Exponent γ dieser Potenz wird der Index von z, in Zeichen

$$\gamma = \text{ind.}\, z$$

genannt, genauer: $\text{ind}_g \cdot z$, da er von der besonderen Wahl der primitiven Wurzel im allgemeinen abhängig ist. In der That, ist $\mathfrak{g}$ eine andere primitive Wurzel, so besteht eine Kongruenz:

$$\mathfrak{g} \equiv g^c \equiv g^{\text{ind}_g \cdot \mathfrak{g}},$$

sowie auch umgekehrt eine Kongruenz

$$g \equiv \mathfrak{g}^k \equiv \mathfrak{g}^{\text{ind}_\mathfrak{g} \cdot g},$$

aus beiden zusammengenommen ergiebt sich

$$g \equiv g^{\text{ind}_g \cdot \mathfrak{g} \cdot \text{ind}_\mathfrak{g} \cdot g} \ (\text{mod.}\, p^\alpha \text{ bezw. } 2p^\alpha)$$

und hieraus, da g primitive Wurzel also eine zum Exponenten $p^{\alpha-1} \cdot (p-1)$ gehörige Zahl ist, die Kongruenz

$$\text{ind}_g \cdot \mathfrak{g} \cdot \text{ind}_\mathfrak{g} \cdot g \equiv 1 \ (\text{mod.}\, p^{\alpha-1}(p-1)). \tag{43}$$

Ferner aber folgt aus (42)

$$z \equiv \mathfrak{g}^{\gamma\, \mathrm{ind}_{\mathfrak{g}} \cdot g} \pmod{p^\alpha \text{ bezw. } 2p^\alpha}$$

d. h.

$$(44) \quad \mathrm{ind}_{\mathfrak{g}} \cdot z \equiv \gamma\, \mathrm{ind}_{\mathfrak{g}} \cdot g \equiv \mathrm{ind}_g \cdot z \cdot \mathrm{ind}_{\mathfrak{g}} \cdot g \pmod{p^{\alpha-1}(p-1)}.$$

Diese Formel lehrt, dafs in der That der Index einer Zahl z mit der primitiven Wurzel wechselt, auf welche er sich bezieht, und dafs man aus dem für eine primitive Wurzel g genommenen Index von z den für eine andere primitive Wurzel $\mathfrak{g}$ geltenden findet, indem man jenen mit dem für $\mathfrak{g}$ geltenden Index von g multipliziert und vom Produkte den Rest nimmt (mod. $p^{\alpha-1}$ $(p-1)$). In entsprechender Weise entsteht der erstere Index aus dem zweiten, wenn dieser mit dem für g geltenden Index von $\mathfrak{g}$ multipliziert wird. Der Kongruenz (43) zufolge sind die genannten beiden Multiplikatoren (mod. $p^{\alpha-1}(p-1)$) assoziiert. Nur die Indices von ± 1 sind von der Wahl der primitiven Wurzel unabhängig, Durch Gleichsetzung der Indices von z findet sich nämlich aus (44)

$$(\mathrm{ind}_{\mathfrak{g}} \cdot g - 1) \cdot \mathrm{ind.}\, z \equiv 0 \pmod{p^{\alpha-1}(p-1)};$$

soll diese Beziehung für jede der von $\mathfrak{g}$ verschiedenen primitiven Wurzeln g bestehen, so mufs sie es auch für $g \equiv \mathfrak{g}^{\pi-1}$ (mod. p^α bezw. $2p^\alpha$), wo wieder π zur Abkürzung steht für $p^{\alpha-1}(p-1)$; dann nimmt sie aber die Gestalt an

$$\left(\frac{\pi}{2} - 1\right) \cdot \mathrm{ind.}\, z \equiv 0 \left(\mathrm{mod.}\ \frac{\pi}{2}\right)$$

und wird nur erfüllt, wenn entweder $\mathrm{ind.}\, z = 0$ d. h. $z \equiv 1$, oder $\mathrm{ind.}\, z = \frac{p^{\alpha-1}(p-1)}{2}$ d. h. $z \equiv -1$ ist.

Der betrachtete Übergang von den Indices, welche sich auf eine bestimmte primitive Wurzel beziehen, zu den für eine andere geltenden Indices ist offenbar völlig analog dem Übergange vom Logarithmensystem für eine gegebene Grundzahl zu dem für eine andere Grundzahl geltenden; überhaupt aber erweist sich die Rechnung mit Indices derjenigen mit Logarithmen ganz entsprechend; insbesondere findet z.B. folgender Satz statt: Der Index eines Produkts ist (mod. $p^{\alpha-1}$ $\cdot(p-1)$) kongruent der Summe der Indices seiner einzelnen Faktoren. Es genügt, ihn für ein Produkt zz' zweier Faktoren zu beweisen. Ist aber

$$z \equiv g^{\mathrm{ind.}\, z}, \quad z' \equiv g^{\mathrm{ind.}\, z'},$$

so ergiebt sich

$$zz' \equiv g^{\mathrm{ind.}\, z + \mathrm{ind.}\, z'}$$

und nun, da auch

$$\left.\begin{aligned} zz' &\equiv g^{\mathrm{ind.}\, z + \mathrm{ind.}\, z'} \\ zz' &\equiv g^{\mathrm{ind.}\, zz'} \end{aligned}\right\} \pmod{p^\alpha \text{ bezw. } 2p^\alpha}$$

und g primitive Wurzel ist, in der That

(45) $$\text{ind.}\, zz' \equiv \text{ind.}\, z + \text{ind.}\, z' \pmod{p^{\alpha-1}(p-1)}.$$

Für den einfachen Fall eines ungeraden Primzahlmodulus p nimmt diese Kongruenz die Gestalt an:

(45a) $$\text{ind.}\, zz' \equiv \text{ind.}\, z + \text{ind.}\, z' \pmod{p-1}.$$

Auch (mod. 2) und (mod. 4) ist jeder zum Modulus primen d. i. ungeraden Zahl z in solcher Weise ein Index zugeordnet, da man

$$z \equiv 1^1 \pmod{2}$$

und, jenachdem z von der Form $4k+1$ oder $4k+3$ ist,

$$z \equiv (-1)^0 \text{ oder } z \equiv (-1)^1 \pmod{4}$$

setzen kann.

Für die übrigen Moduln, für welche keine primitive Wurzel vorhanden ist, kommt dagegen einer zum Modulus primen Zahl z nicht in gleicher Weise ein Index zu, wie bisher; aber auch dann läſst sich eine entsprechende, nur weniger einfache Beziehung aufstellen. In der That, wenn zunächst $n = 2^\lambda$, $\lambda > 2$ ist, so ist jede zu n prime Zahl z einer bestimmten der Potenzen (32) kongruent, man darf also setzen:

(46) $$z \equiv (-1)^\alpha \cdot 5^\beta \pmod{2^\lambda},$$

wo α ein bestimmter der Werte 0, 1 und β eine bestimmte der Zahlen $0, 1, 2, \ldots 2^{\lambda-2}-1$ ist; dies gilt sogar noch für $\lambda = 2$, sodaſs der Modulus 4 hier subsumiert werden kann, wie schlieſslich auch der Modulus 2, wenn man dann α, β gleich Null festsetzt. Man hat hier zwar nicht **einen Index** für die Zahl z, wohl aber ein bestimmtes **System zweier Indices**, die Exponenten α und β.

Ist endlich $n = 2^\lambda p'^{\alpha'} p''^{\alpha''} \ldots$ ein ganz beliebiger Modulus und z eine zu ihm relativ prime Zahl, so bestehen dem Gesagten zufolge, wenn $g', g'', \ldots$ primitive Wurzeln für die Moduln $p'^{\alpha'}, p''^{\alpha''}, \ldots$ resp. bedeuten, Kongruenzen von der Eorm

(47) $$\begin{aligned} z &\equiv (-1)^\alpha \cdot 5^\beta \pmod{2^\lambda} \\ z &\equiv g'^{\gamma'} \pmod{p'^{\alpha'}} \\ z &\equiv g''^{\gamma''} \pmod{p''^{\alpha''}} \\ &\ldots\ldots\ldots\ldots, \end{aligned}$$

in denen $\alpha, \beta, \gamma', \gamma'' \ldots$ bestimmte Werte resp. aus den Reihen

$$0,1;\ 0,1,2,\ldots 2^{\lambda-2}-1;\ 1,2,\ldots p'^{\alpha'-1}(p'-1);\ 1,2,\ldots p''^{\alpha''-1}(p''-1);\ldots$$

sind. Diese bestimmten Exponenten $\alpha, \beta, \gamma', \gamma'', \ldots$ dürfen zusammengenommen **die Indices von z** genannt werden, sodaſs es in diesem allgemeinsten Falle wieder zwar nicht einen Index, wohl aber ein System mehrerer Indices für die Zahl z

giebt. Demselben kommt eine analoge Eigenschaft zu, wie sie für den Fall eines Modulus p^α oder $2p^\alpha$ in der Kongruenz (45) sich ausspricht. Sind nämlich

$$\alpha,\ \beta,\ \gamma',\ \gamma'',\ \ldots$$
$$\alpha_1, \beta_1, \gamma_1', \gamma_1'', \ldots$$

die Indices zweier Zahlen z, z_1, und sind

$$\alpha_2,\ \beta_2,\ \gamma_2',\ \gamma_2'',\ \ldots$$

die Indices ihres Produktes zz_1, so bestehen die Kongruenzen

$$(48)\quad \begin{gathered} \alpha_2 \equiv \alpha + \alpha_1 \ (\text{mod. } 2), \quad \beta_2 \equiv \beta + \beta_1 \ (\text{mod. } 2^{\lambda-2}) \\ \gamma_2' \equiv \gamma' + \gamma_1' (\text{mod.} p'^{\alpha'-1}(p'-1)),\ \gamma_2'' \equiv \gamma'' + \gamma_1'' (\text{mod.} p''^{\alpha''-1}(p''-1)), \ldots \end{gathered}$$

Dies folgt für die Indices γ_2', γ_2'', ... sofort aus (45); ferner aber erschliefst man aus den Kongruenzen

$$z \equiv (-1)^\alpha 5^\beta,\ z_1 \equiv (-1)^{\alpha_1} 5^{\beta_1} \ (\text{mod. } 2^\lambda)$$

die andere:

$$zz_1 \equiv (-1)^{\alpha+\alpha_1} \cdot 5^{\beta+\beta_1},$$

also in Verbindung mit der Kongruenz

$$zz_1 \equiv (-1)^{\alpha_2} \cdot 5^{\beta_2}$$

die folgende:

$$(-1)^{\alpha_2} \cdot 5^{\beta_2} \equiv (-1)^{\alpha_0} \cdot 5^{\beta_0},$$

wenn α_0, β_0 die kleinsten Reste von $\alpha + \alpha_1$, $\beta + \beta_1$ (mod. 2) resp. (mod. $2^{\lambda-2}$) bedeuten. Hier steht beiderseits eine der Potenzen (32), welche nur kongruent sein können, wenn sie identisch sind, also ist $\alpha_2 = \alpha_0$, $\beta_2 = \beta_0$, mithin die ersten beiden der Kongruenzen (48) ebenfalls erfüllt.

9. Bei der grofsen Bedeutung, welche den vorstehenden Entwicklungen zufolge den primitiven Wurzeln einer Primzahl p zukommt, ist es wichtig, sich klar zu machen, wie man in jedem Falle eine solche ermitteln könne. Man setze zu diesem Zwecke wieder

$$p - 1 = a^\alpha b^\beta c^\gamma \ldots;$$

dann mufs eine Zahl z, welche nicht primitive Wurzel (mod. p) d. h. keine primitive Wurzel der Kongruenz

$$z^{p-1} \equiv 1 \ (\text{mod. } p)$$

ist, einer Kongruenz von derselben Gestalt, deren Exponent ein Teiler von $p-1$ ist, mithin wenigstens einer der folgenden Kongruenzen:

$$z^{\frac{p-1}{a}} \equiv 1,\ z^{\frac{p-1}{b}} \equiv 1,\ z^{\frac{p-1}{c}} \equiv 1 \ldots (\text{mod. } p)$$

genügen, und umgekehrt wird eine Zahl z, die eine dieser Kongruenzen, etwa die erste derselben erfüllt, nicht zum Exponenten $p-1$ gehören

also keine primitive Wurzel (mod. p) sein können. Nun sind, wie wir demnächst sehen werden, die Wurzeln dieser Kongruenzen resp. die a^{ten}, b^{ten}, $c^{\text{ten}}, \ldots$ Potenzreste (mod. p). Scheidet man daher aus der Reihe

$$(49) \qquad 1, 2, 3, \ldots p-1$$

successive die Zahlen aus, welche a^{te} Potenzreste sind, aus den überbleibenden Zahlen diejenigen, welche b^{te} Potenzreste sind u. s. w., so müssen notwendig diejenigen Zahlen, welche zuletzt verbleiben, die primitiven Wurzeln (mod. p) sein.

Diese nicht sehr praktische Methode läfst sich nach Gaufs (*D. A. art.* 73) auf Grund des in Nr. 3 gegebenen Hilfssatzes durch folgende andere ersetzen.

Man greife aus der Reihe (49) irgend eine Zahl z heraus und bilde (Nr. 1) ihre Periode d. h. die Potenzen $1, z, z^2, \ldots$, bis man zu einer Potenz z^δ gelangt, welche (mod. p) den Rest 1 giebt; z gehört dann (mod. p) zum Exponenten δ, der ein Teiler von $p-1$ sein mufs (Nr. 1), die Potenzen

$$(50) \qquad 1, z, z^2, \ldots z^{\delta-1}$$

sind die sämtlichen Wurzeln der Kongruenz $z^\delta \equiv 1$ (mod. p) und sie enthalten daher unter sich auch die sämtlichen nicht primitiven Wurzeln dieser Kongruenz d. h. (Nr. 2) sämtliche Zahlen, welche zu einem Teiler von δ als Exponenten gehören. Fände sich nun $\delta = p-1$, so hätte man bereits in z eine primitive Wurzel (mod. p) ermittelt. Ist dagegen $\delta < p-1$, so sei z' eine Zahl, welche keiner der Potenzen (50) kongruent ist; man bilde für diese wieder ihre Periode

$$1, z', z'^2, \ldots z'^{\delta'-1},$$

wo δ' den Exponenten bedeutet, zu dem z' gehört; er kann, wie soeben bemerkt, kein Teiler von δ sein und demnach mufs das kleinste gemeinsame Vielfache δ_1 von δ, δ' gröfser als δ sein. Man zerlege nun (s. Kap. 2, Nr. 9) die Zahl δ_1 nach der Formel $\delta_1 = dd'$ in der Weise in zwei relativ prime Faktoren, dafs d in δ, d' in δ' aufgehe. Da $z^{\frac{\delta}{d}}$ zur d^{ten}, offenbar aber zu keiner kleineren Potenz erhoben kongruent 1 wird (mod. p), so gehört $z^{\frac{\delta}{d}}$ zum Exponenten d, ebenso $z'^{\frac{\delta'}{d'}}$ zum Exponenten d'; nach dem in Nr. 3 benutzten Hilfssatze gehört folglich $z_1 = z^{\frac{\delta}{d}} \cdot z'^{\frac{\delta'}{d'}}$ zum Exponenten $\delta_1 > \delta$. Wäre die so bestimmte Zahl $\delta_1 = p-1$, so hätte man jetzt in z_1 eine primitive Wurzel (mod. p) ermittelt, andernfalls gäbe es eine Zahl, welche keiner der Potenzen

$$1, z_1, z_1^2, \ldots z_1^{\delta_1-1}$$

kongruent wäre, und man könnte dann genau wie soeben eine Zahl z_2 ermitteln, welche zu einem noch gröfseren Exponenten δ_2 als δ_1 gehörte, u. s. w. Fährt man aber so fort, so mufs in der wachsenden Reihe der Zahlen $\delta, \delta_1, \delta_2, \ldots$, welche sämtlich Teiler von $p-1$ sind, endlich eine gleich $p-1$ werden, womit dann in der zugehörigen der Zahlen $z, z_1, z_2, \ldots$ eine primitive Wurzel (mod. p) gefunden sein würde.

Sei z. B. $p = 41$. Wählt man $z = 2$, so findet sich als zugehörige Periode die folgende Reihe von Zahlen:

$$1, 2, 4, 8, 16, 32, 23, 5, 10, 20, 40, 39, 37, 33, 25, 9, 18, 36, 31, 21,$$

also $\delta = 20$. Da noch $\delta < p-1$, so wähle man für z' einen der Reste (mod. 41), welche sich in der vorstehenden Reihe nicht finden, etwa $z' = 3$; die zugehörige Periode ist folgende Reihe von Zahlen:

$$1, 3, 9, 27, 40, 38, 32, 14,$$

mithin $\delta' = 8$. Demnach findet sich $\delta_1 = \frac{20 \cdot 8}{4} = 40 = 5 \cdot 8$, und somit $z_1 = 2^4 \cdot 3^1 \equiv 7$ (mod. 41) als primitive Wurzel dieses Modulus.*)

10. Wir kehren nunmehr zur Kongruenz (1) wieder zurück und versuchen, sie aufzulösen. Sei

$$n = 2^\lambda p'^{\alpha'} p''^{\alpha''} \ldots \tag{51}$$

Wenn die Kongruenz (1) auflösbar und $x \equiv \xi$ (mod. n) eine Lösung derselben, also $\xi^m \equiv a$ (mod. n) ist, so ist ξ auch eine Wurzel jeder der Kongruenzen

$$x^m \equiv a \text{ (mod. } 2^\lambda), \quad x^m \equiv a \text{ (mod. } p'^{\alpha'}), \ldots \tag{52}$$

und demnach ist die Kongruenz (1) unlösbar, sobald auch nur eine der letzteren Kongruenzen es ist, sobald also a auch nur in Bezug auf einen der Moduln $2^\lambda, p'^{\alpha'}, p''^{\alpha''}, \ldots$ m^{ter} Nichtrest ist. Wenn dagegen a für jeden derselben ein m^{ter} Potenzrest ist, die Kongruenzen (52) mithin alle auflösbar sind, und es bedeuten $\varrho, \sigma, \tau, \ldots$ je eine Wurzel derselben, $r, s, t, \ldots$ aber die aus Kap. 3, Nr. 8 hinreichend bekannten Hilfszahlen, so wird die Zahl

$$\xi \equiv r\varrho + s\sigma + t\tau \ldots \text{ (mod. } n) \tag{53}$$

eine Wurzel der Kongruenz (1) repräsentieren; denn, da aus der vorstehenden Formel sich

$$\xi \equiv \varrho \text{ (mod. } 2^\lambda), \quad \xi \equiv \sigma \text{ (mod. } p'^{\alpha'}), \ldots$$

ergiebt, so findet sich

$$\xi^m \equiv a \text{ (mod. } 2^\lambda), \quad \xi^m \equiv a \text{ (mod. } p'^{\alpha'}), \ldots$$

also auch

$$\xi^m \equiv a \text{ (mod. } n).$$

---

*) Eine Tabelle der kleinsten primitiven Wurzeln aller Primzahlen < 3000 hat neuerdings G. Wertheim (*Acta Math.* 17, 1893, p. 315) veröffentlicht.

Setzt man daher in diesem Falle in der Formel (53) für $\varrho, \sigma, \tau, \ldots$ der Reihe nach alle möglichen Wurzeln der abgeleiteten Kongruenzen (52) ein, so erhält man die sämtlichen Wurzeln von (1) und sie allein, deren Anzahl also der Anzahl jener Wurzelkombinationen gleich ist. Bezeichnen $w(2^\lambda)$, $w(p'^{\alpha'})$, ... die Anzahl der Wurzeln der einzelnen Kongruenzen (52), sodafs z. B. $w(2^\lambda) = 0$ zu setzen ist, falls a ein m^{ter} Nichtrest (mod. 2^λ), so wird hiernach die Anzahl $w(n)$ der Wurzeln von (1) jederzeit durch die Formel

$$w(n) = w(2^\lambda) \cdot w(p'^{\alpha'}) \cdot w(p''^{\alpha''}) \ldots$$

gegeben sein.

Demgemäfs erübrigt nur die nähere Betrachtung der Kongruenz

$$x^m \equiv a \pmod{2^\lambda} \tag{54}$$

sowie einer Kongruenz

$$x^m \equiv a \pmod{p^\alpha}, \tag{55}$$

deren Modulus die Potenz einer ungeraden Primzahl ist.

Mit der Untersuchung der letzteren wollen wir beginnen.

Den allgemeinen Betrachtungen in Nr. 1 zufolge hat diese Kongruenz genau dieselben Wurzeln wie die andere:

$$x^\delta \equiv a \pmod{p^\alpha}, \tag{56}$$

in welcher δ gröfster gemeinsamer Teiler ist von m und $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$. Setzt man aber a als m^{ten} Potenzrest (mod. p^α) voraus, so hat nach derselben Nummer die letztgeschriebene Kongruenz ebensoviel Wurzeln, wie die Kongruenz

$$z^\delta \equiv 1 \pmod{p^\alpha} \tag{57}$$

d. h. nach Nr. 4 genau δ. Werden nun die $\varphi(p^\alpha)$ Glieder eines reduzierten Restsystems (mod. p^α) zur m^{ten} Potenz erhoben, so gehen sämtliche inkongruente m^{te} Potenzreste (mod. p^α) und dem eben Bemerkten zufolge jeder von ihnen δ Mal hervor. Daher mufs es

$$d = \frac{\varphi(p^\alpha)}{\delta}$$

inkongruente m^{te} Potenzreste (mod. p^α) geben.

Ist z. B. $m = 2$, handelt es sich also um quadratische Reste (mod. p^α), so findet sich $\delta = 2$, die Anzahl dieser quadratischen Reste also gleich $\frac{p^{\alpha-1}(p-1)}{2}$. Ebenso grofs ist unterhalb p^α die Anzahl der quadratischen Reste (mod. p), und man überzeugt sich leicht, dafs diese letzteren auch **identisch** sind mit den ersteren, denn für jede Zahl a, für welche die Kongruenz $x^2 \equiv a$ (mod. p^α) möglich ist, wird auch die einfachere: $x^2 \equiv a$ (mod. p) erfüllt.

Ob nun eine Zahl a m^{ter} Potenzrest (mod. p^α) ist, oder nicht, kann durch ein theoretisch sehr einfaches Kriterium entschieden werden. Besteht nämlich die Kongruenz (56), so erhält man durch ihre Erhebung zur $\frac{\varphi(p^\alpha)}{\delta}^{\text{ten}}$ Potenz mit Rücksicht auf den Fermatschen Satz d. i. auf die Kongruenz

$$x^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha}$$

die Beziehung

$$a^{\frac{\varphi(p^\alpha)}{\delta}} \equiv 1 \pmod{p^\alpha}. \tag{58}$$

Jeder der $\frac{\varphi(p^\alpha)}{\delta}$ m^{ten} Potenzreste (mod. p^α) ist also eine Wurzel der Kongruenz

$$z^{\frac{\varphi(p^\alpha)}{\delta}} \equiv 1 \pmod{p^\alpha};$$

da letztere aber (nach Nr. 4) genau $\frac{\varphi(p^\alpha)}{\delta}$ Wurzeln hat, so kann ihr auch keine weitere Zahl genügen, und demnach besteht die Beziehung (58) nicht für m^{te} Nichtreste a. Somit findet sich der Satz: Eine Zahl a ist m^{ter} Potenzrest (mod. p^α) oder nicht, jenachdem die Bedingung (58) erfüllt oder nicht erfüllt ist.

Ist z. B. m also auch δ gleich 2, so erhält man als Bedingung für die quadratischen Reste a (mod. p^α) die Kongruenz

$$a^{p^{\alpha-1}\cdot\frac{p-1}{2}} \equiv 1 \pmod{p^\alpha};$$

demnach ist -1 quadratischer Rest oder Nichtrest (mod. p^α), jenachdem

$$(-1)^{p^{\alpha-1}\cdot\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p^\alpha}$$

d. h. gleich 1 ist oder nicht, oder also, jenachdem p die Form $4k+1$ oder die Form $4k-1$ hat.

Sei noch $m=4$; dann ist $\delta=4$ oder $\delta=2$, jenachdem p von der Form $4k+1$ oder $4k-1$ ist. Demgemäfs nimmt der Ausdruck $a^{\frac{\varphi(p^\alpha)}{\delta}}$ für $a=-1$ im letzteren Falle die Gestalt

$$(-1)^{p^{\alpha-1}\cdot\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} = -1$$

an und zeigt so, dafs -1 biquadratischer Nichtrest ist. Im ersteren Falle wird für $a=-1$ jener Ausdruck

$$(-1)^{p^{\alpha-1}\cdot\frac{p-1}{4}} = (-1)^{\frac{p-1}{4}}$$

kongruent $+1$ oder -1, jenachdem p von der Form $8h+1$ oder $8h+5$ ist, und deshalb ist -1 für die Primzahlen von der ersteren

Form biquadratischer Rest, für diejenigen der zweiten Form biquadratischer Nichtrest (vgl. Gaufs, *theor. resid. biquadr.* I *art.* 9).

Allgemein ergiebt sich offenbar aus der Bedingung (58), welche die m^{ten} Potenzreste (mod. p^α) charakterisiert, das Resultat, dafs das Produkt zweier m^{ten} Potenzreste wieder ein m^{ter} Potenzrest, das Produkt aus einem m^{ten} Potenzreste und einem m^{ten} Nichtreste dagegen ein m^{ter} Nichtrest sein mufs. Wie es sich mit einem Produkte zweier m^{ten} Nichtreste verhalte, geht allgemein nicht, wie es bei den quadratischen Resten geschah, aus jener Bedingung hervor. Da die Anzahl $d = \frac{\varphi(p^\alpha)}{\delta}$ der inkongruenten m^{ten} Potenzreste (mod. p^α) ein Teiler von $\varphi(p^\alpha)$ ist, giebt es (nach Nr. 4) genau $\varphi(d)$ Zahlen a, welche (mod. p^α) zum Exponenten d gehören; jede dieser Zahlen aber genügt der Kongruenz (58), ist also ein m^{ter} Potenzrest, und da somit die (mod. p^α) inkongruenten d Potenzen $1, a, a^2, \ldots a^{d-1}$ ebenfalls m^{te} Potenzreste sind, so stellt diese Reihe von Potenzen die sämtlichen m^{ten} Potenzreste dar.

Ihre Summe ist

$$1 + a + a^2 + \cdots + a^{d-1} = \frac{a^d - 1}{a - 1}.$$

Nun kann, wenn m durch $p-1$ nicht aufgeht, nicht $a \equiv 1 \pmod{p}$ sein, weil hieraus nach dem Hilfssatze der Nr. 4 die Kongruenz

$$a^{p^{\alpha-1}} \equiv 1 \pmod{p^\alpha}$$

hervorginge, welche mit der vorausgesetzten Kongruenz

$$a^d \equiv 1 \pmod{p^\alpha}$$

verbunden, die fernere:

$$a^t \equiv 1 \pmod{p^\alpha}$$

ergäbe, in welcher t den gröfsten gemeinsamen Teiler von $p^{\alpha-1}$ und d bedeutet; dieser wäre aber kleiner als d, da $d = \frac{p^{\alpha-1}(p-1)}{\delta}$ kein Teiler von $p^{\alpha-1}$ ist, und somit widerspräche die vorige Kongruenz der Bedeutung von a. Hieraus folgt, dafs die rechte Seite der letzten Gleichung dann durch p^α teilbar, andernfalls aber, wie leicht zu übersehen, es nicht ist. Man findet also den Satz:

Die Summe der m^{ten} Potenzreste (mod. p^α) ist kongruent Null oder nicht kongruent Null, jenachdem m durch $p-1$ teilbar oder nicht teilbar ist.

Ihr Produkt findet sich durch den Ausdruck

$$a^{1+2+\cdots+(d-1)} = a^{\frac{d(d-1)}{2}}.$$

Wenn hier d ungerade ist, so wird

$$(a^d)^{\frac{d-1}{2}} \equiv 1 \pmod{p^\alpha};$$

ist dagegen d gerade, also $d-1$ ungerade und

$$a^d - 1 = \left(a^{\frac{d}{2}} - 1\right)\left(a^{\frac{d}{2}} + 1\right) \equiv 0 \pmod{p^\alpha},$$

wo nur einer der Faktoren durch p teilbar sein kann, da ihre Differenz es nicht ist, so folgt nach der Bedeutung der Zahl a

$$a^{\frac{d}{2}} \equiv -1 \pmod{p^\alpha}$$

und folglich

$$\left(a^{\frac{d}{2}}\right)^{d-1} \equiv (-1)^{d-1} \equiv -1 \pmod{p^\alpha}.$$

So erhält man den ferneren Satz: Das Produkt der m^{ten} Potenzreste $(\text{mod.}\, p^\alpha)$ ist kongruent 1 oder -1, jenachdem $\frac{\varphi(p^\alpha)}{\delta}$ ungerade oder gerade ist.

Endlich bemerken wir, dafs das Kriterium (58) mit Hilfe der Theorie der Indices (Nr. 8) durch ein anderes, äquivalentes ersetzt werden kann. Besteht nämlich die Kongruenz (55), so führt die Bemerkung, dafs zwei $(\text{mod.}\, p^\alpha)$ kongruente Zahlen den gleichen Index haben, der Index eines Produktes aber $(\text{mod.}\, \varphi(p^\alpha))$ der Summe der Indices der Faktoren kongruent ist, zur folgenden Kongruenz

$$m \cdot \text{ind.}\, x \equiv \text{ind.}\, a \pmod{\varphi(p^\alpha)}, \tag{59}$$

welche in Bezug auf die Gröfse ind. x vom ersten Grade ist. Nach der Theorie solcher Kongruenzen ist dieselbe dann und nur dann auflösbar, wenn der gröfste gemeinsame Teiler von m, $\varphi(p^\alpha)$ d. i. die Zahl δ auch in ind. a aufgeht; unter dieser Bedingung aber giebt es dann δ Werte ξ des ind. x, welche die Kongruenz erfüllen, und jedem von ihnen entspricht durch die Formel

$$x \equiv g^\xi \pmod{p^\alpha},$$

in welcher g die dem gedachten Indexsysteme zum Grunde liegende primitive Wurzel $(\text{mod.}\, p^\alpha)$ bedeutet, eine Wurzel der Kongruenz (55).

Hiernach ist eine Zahl a m^{ter} Potenzrest $(\text{mod.}\, p^\alpha)$ dann und nur dann, wenn

$$\text{ind.}\, a \equiv 0 \pmod{\delta} \tag{60}$$

ist.

Zugleich lehrt die angestellte Betrachtung eine Methode zur Auflösung der Kongruenz (55) für den Fall, dafs diese für a erforderliche Bedingung erfüllt ist. Man denke sich für eine beliebig gewählte primitive Wurzel g $(\text{mod.}\, p^\alpha)$ eine

Tabelle*) aufgestellt, welche für alle Glieder eines reduzierten Restsystems die zugehörigen Indices angiebt, und wieder eine zweite Tabelle — die umgekehrte der ersteren —, aus welcher für jeden Wert des Index d. h. für die Zahlen $1, 2, 3, \ldots \varphi(p^\alpha)$ die ihnen entsprechenden Glieder des reduzierten Restsystems zu entnehmen sind, genau wie eine Logarithmentafel für jede Zahl den entsprechenden Logarithmus, aber auch für jeden Logarithmus die zugehörige Zahl auffinden läfst. Um dann die Kongruenz (55) zu lösen, betrachte man die ihr äquivalente Kongruenz (59). Diese ist unter der Bedingung (60), deren wirkliches Stattfinden durch die erste Tabelle festgestellt werden kann, auflösbar. Man suche demgemäfs die Lösungen der Kongruenz

$$mz \equiv \text{ind. } a \pmod{\varphi(p^\alpha)},$$

deren Anzahl gleich δ ist, und nenne sie

$$z_1, z_2, \ldots z_\delta; \tag{61}$$

die Zahlen

$$x_1, x_2, \ldots x_\delta,$$

welche nach der zweiten Tabelle den Indices (61) entsprechen, sind dann die δ Wurzeln der Kongruenz (55).

11. Nunmehr wenden wir uns noch zur Betrachtung der Kongruenz (54).

Die Fälle $\lambda = 1$ und $\lambda = 2$ erledigen sich ohne weiteres. Der einzige ungerade Rest a (mod. 2) ist $a = 1$, die Kongruenz

$$x^m \equiv 1 \pmod{2}$$

aber ist stets auflösbar und hat die einzige Wurzel $x \equiv 1$.

Als ungerade Reste a (mod. 4) dürfen $a = +1$, $a = -1$ gewählt werden. Ist nun zunächst m ungerade, so ist die Kongruenz

$$x^m \equiv \pm 1 \pmod{4},$$

da für eine ungerade Zahl x stets $x^2 \equiv 1$ (mod. 4) ist, mit der einfacheren:

$$x \equiv \pm 1 \pmod{4}$$

identisch und hat also die einzige Wurzel $x \equiv +1$ resp. $x \equiv -1$ (mod. 4). Für ein gerades m dagegen ist

$$x^m \equiv -1 \pmod{4}$$

unmöglich, während

---

*) Für den Fall eines einfachen Primzahlmodulus p gab bereits Gaufs (*D. A. tab.* I) eine kleine, bis $p = 97$ gehende Tafel. S. ferner C. G. J. Jacobi's *Canon arithmeticus*, *Regiomontanae* 1839, in welchem u. a. die gedachten zwei sich ergänzenden Tabellen in gröfserem Umfange für Primzahlmoduln aufgestellt sind. Vgl. auch V. A. Lebesgue, *Journ. de math.* 19, 1854, p. 334.

$$x^m \equiv +1 \pmod{4}$$

die zwei Wurzeln $x \equiv 1$, $x \equiv -1$ zuläfst.

Sei jetzt $\lambda > 2$ und $\delta = 2^{\lambda-\nu}$ der gröfste gemeinsame Teiler von m und $2^{\lambda-2}$. Nach Nr. 1 hat die Kongruenz (54), falls sie überhaupt lösbar also a m^{ter} Potenzrest (mod. 2^λ) ist, ebensoviel Wurzeln, wie die Kongruenz

$$z^m \equiv 1 \pmod{2^\lambda}.$$

Für jede der stets ungeraden Lösungen z der letzteren besteht aber auch die Kongruenz (31):

$$z^{2^{\lambda-2}} \equiv 1 \pmod{2^\lambda}$$

also genügt jede derselben auch der Kongruenz

$$z^{2^{\lambda-\nu}} \equiv 1 \pmod{2^\lambda} \tag{62}$$

und umgekehrt. Letztere Kongruenz hat, wenn $\nu = \lambda$ d. h. $\delta = 1$ ist, was dann und nur dann der Fall sein wird, wenn m eine ungerade Zahl bedeutet, nur eine Wurzel $z \equiv 1$, andernfalls hat sie deren (nach Nr. 5) $2 \cdot 2^{\lambda-\nu} = 2^{\lambda-\nu+1}$. Da nun die $2^{\lambda-1}$ ungeraden Reste (mod. 2^λ), zur m^{ten} Potenz erhoben, die sämtlichen m^{ten} Potenzreste a ergeben und jeden von ihnen so oft, als die Anzahl Wurzeln der Kongruenz (54) oder (62) beträgt, so findet sich die Anzahl aller m^{ten} Potenzreste (mod. 2^λ) je nach den soeben unterschiedenen Fällen: nämlich für ein ungerades m gleich $2^{\lambda-1}$ (d. h. jede ungerade Zahl ist dann m^{ter} Potenzrest (mod. 2^λ)), für ein gerades m dagegen gleich $2^{\nu-2}$.

Ob aber im letzteren Falle eine ungerade Zahl a m^{ter} Potenzrest (mod. 2^λ) sei oder nicht, könnte man suchen vermittelst der Kongruenz (54) analog zu entscheiden, wie dieselbe Frage in Bezug auf den Modulus p^α mittels der Kongruenz (56) entschieden worden ist. Besteht nämlich jene Kongruenz, so findet sich daraus durch Erhebung in die $2^{\nu-2}$te Potenz

$$a^{2^{\nu-2}} \equiv 1 \pmod{2^\lambda}, \tag{63}$$

eine Bedingung, der mithin jeder m^{te} Potenzrest (mod. 2^λ) Genüge leisten mufs. Hier ist aber diese notwendige Bedingung nicht, wie bei dem aus (56) abgeleiteten Kriterium (58), zugleich auch die ausreichende Bedingung dafür, dafs a m^{ter} Potenzrest sei; denn es giebt, wie gezeigt, nur $2^{\nu-2}$ m^{te} Potenzreste (mod. 2^λ), die Kongruenz

$$x^{2^{\nu-2}} \equiv 1 \pmod{2^\lambda} \tag{64}$$

dagegen hat, falls nicht $\nu = 2$ ist, $2 \cdot 2^{\nu-2}$ Wurzeln. Hier zerfallen dann also die ungeraden Zahlen (mod. 2^λ) in drei Klassen, welche enthalten:

1) Die $2^{\nu-2}$ m^{ten} Potenzreste; 2) diejenigen $2^{\nu-2}$ m^{ten} Nichtreste, welche der Kongruenz (64) genügen, und 3) die übrigen m^{ten} Nichtreste.

Ist $\nu = 2$, mithin nur ein m^{ter} Potenzrest, nämlich die Zahl $a \equiv 1 \pmod{2^\lambda}$ vorhanden, so hat auch die Kongruenz (64) nur eine Wurzel, die zweite Klasse bleibt leer, und jeder von 1 verschiedene ungerade Rest (mod. 2^λ) gehört der dritten Klasse an.

Um in dem interessanteren Falle $\nu > 2$ die Verteilung der ungeraden Zahlen a (mod. 2^λ) in die angegebenen drei Klassen näher zu übersehen, denke man sich jene Zahlen nach dem Exponenten gruppiert, zu welchem sie (mod. 2^λ) gehören. Sei also a eine zum Exponenten $2^{\lambda-\mu}$ gehörige Zahl. Nach Nr. 5 haben derartige Zahlen (mod. 2^λ) die Form $\pm 5^{2^{\mu-2}u}$, wo u ungerade ist; nach derselhen Nummer findet sich

$$5^{2^{\mu-2}} = 1 + 2^\mu \cdot h$$

also auch

$$\pm 5^{2^{\mu-2}\cdot u} = \pm 1 + 2^\mu \cdot k,$$

wo h, k ungerade Zahlen bedeuten; also hat jede zum Exponenten $2^{\lambda-\mu}$ gehörige Zahl auch diese letztere Form. Umgekehrt ist aber auch jede Zahl von der Form $\pm 1 + 2^\mu k$, wo k ungerade ist, eine zum Exponenten $2^{\lambda-\mu}$ gehörige Zahl. Denn, wenn zunächst $a = 1 + 2^\mu k$ also $a - 1$ genau durch 2^μ teilbar ist, so ist nach dem (auch für $p = 2$ giltigen) Hilfssatze der Nr. 4

$$a^{2^{\lambda-\mu}} - 1$$

genau durch 2^λ und demnach nicht schon

$$a^{2^{\lambda-\mu-1}} - 1$$

durch 2^λ teilbar. Ist dagegen $a = -1 + 2^\mu k$, so ist $a^2 - 1$ genau durch $2^{\mu+1}$ teilbar, woraus wieder dieselbe Folgerung hervorgeht. Da μ mindestens $= 2$ ist, giebt es unter den ungeraden Zahlen (mod. 2^λ) offenbar ebensoviel Zahlen der Form $1 + 2^\mu k$, wie Zahlen der Form $-1 + 2^\mu k$.

Damit nun eine solche, der Kongruenz $x^{2^{\lambda-\mu}} \equiv 1 \pmod{2^\lambda}$ genügende Zahl a auch die Bedingung (64) erfüllt, ist notwendig und hinreichend, dafs $2^{\nu-2}$ ein Vielfaches von $2^{\lambda-\mu}$, also $\nu - 2 \geqq \lambda - \mu$ oder $\mu \geqq \lambda - \nu + 2$ sei.

Ist folglich $\mu < \lambda - \nu + 2$, so finden sich sämtliche zum Exponenten $2^{\lambda-\mu}$ gehörige Zahlen in der dritten Klasse.

Im entgegengesetzten Falle verteilen sich die letztgenannten Zahlen in der Weise auf die beiden ersten Klassen, dafs diejenigen von der Form $1 + 2^\mu k$ der ersten, diejenigen von der Form $-1 + 2^\mu k$ der zweiten angehören. Um sich hiervon zu überzeugen, bemerke man einerseits, dafs die Zahlen

$$1 + 2^\mu k, \quad -1 + 2^\mu k,$$

welche den sämtlichen zulässigen Werten μ der gedachten Art, nämlich den durch die Ungleichheiten $\lambda \overline{\gtrless} \mu \overline{\gtrless} \lambda - \nu + 2$ bestimmten μ entsprechen, die sämtlichen Wurzeln der Kongruenz (64) ausmachen, zur Hälfte also der ersten, zur Hälfte der zweiten Klasse angehören; andererseits, dafs eine Zahl der zweiten Form kein m^{ter} Potenzrest (mod. 2^λ) sein kann, denn, wäre

$$x^m \equiv -1 + 2^\mu k \pmod{2^\lambda},$$

so folgte, da μ mindestens $= 2$ ist, $x^m \equiv -1 \pmod{4}$, was nicht sein kann, da x ungerade und m gerade ist. Da nun die Menge der Zahlen $-1 + 2^\mu k$ ebenso zahlreich ist, wie diejenigen der Zahlen $1 + 2^\mu k$, müssen die Zahlen der letztern Form zur ersten Klasse gehören.

Auf die vorstehend, zumeist im Anschlusse an die Arbeit von C. F. Arndt (*Journ. f. Math.* 31, 1846, p. 333) gegebenen Bemerkungen über die m^{ten} Potenzreste müssen wir uns hier beschränken, da die eingehendere Theorie der letzteren nur aus Betrachtungen geschöpft werden kann, welche weit über die Grenzen der „Niederen Zahlentheorie“ hinausgreifen.*)

12. An die Theorie der Potenzreste schliefst sich passend die Entwicklung rationaler Brüche in Dezimalbrüche an, die wir hier in ihren Hauptzügen als besonderen Fall einer allgemeineren Entwicklungsart herleiten wollen.**)

Im 2. Kapitel Nr. 11 ist gezeigt worden, dafs jede positive ganze Zahl mittels einer gegebenen Grundzahl, die hier g genannt werden mag, in die Gestalt

$$ag^h + a_1 g^{h-1} + \cdots + a_{h-1} g + a_h \tag{65}$$

gesetzt werden kann, in welcher $a, a_1, \ldots a_{h-1}, a_h$ positive ganze Zahlen $< g$ oder Null sind. Dasselbe wird in gleicher Weise für jeden positiven Wert überhaupt als richtig erkannt, nur dafs alsdann a_h keine ganze Zahl, sondern, wenn wir uns hier auf die Entwicklung rationaler Werte beschränken, nur eine rationale Zahl $< g$ sein

*) S. zu den voraufgehenden Nummern aufser der angeführten Arbeit von Arndt die *artt.* 45—93 der *Disqu. Arithm.* von Gaufs, sowie seine nachgelassene Arbeit *solutio congruentiae* $X^m - 1 \equiv 0$, *Werke* II, p. 199, desgl. J. A. Serret, *Handb. der höheren Algebra*, deutsch v. Wertheim II, 2. Kap. — Vgl. auch Euler, *theor. circa residua ex divisione potest. relicta*, *Comm. N. Petr.* 7, p. 49; *Dem. circa residua etc.*, ibidem 18, p. 85; *Opusc. analyt.* I *dissert.* 5 und 8.

**) Weiteres darüber sehe man u. a. bei S. Morel und E. Pellet, *Nouv. Ann. de Math.* (2) 10, 1871, p. 39 u. 93; J. W. L. Glaisher, *Henry Goodwyn's table of circles*, Proceed. Cambridge 3, 1879, p. 195; Th. Schröder, *Progr. d. Gymn. zu Ansbach* 1872; J. Hartmann, *Pr. d. G. zu Rinteln* 1872; Kessler, *Periodenlängen der Dezimalbrüche,* Berlin 1895.

wird. Eine solche aber ist stets die Summe aus einer ganzen Zahl, die $< g$ ist und auch Null sein kann, und einem echten Bruche $\frac{r}{n}$, welch' letzteren man als reduziert annehmen darf, sodafs r eine der relativen Primzahlen zu n ist, welche kleiner als n sind. Jeder Bruch dieser Art, deren es $\varphi(n)$ bei gegebenem Nenner n giebt, verstattet nun eine Entwicklung ähnlicher Art wie die Entwicklung (65), die jedoch nach den negativen Potenzen von g fortschreitet. Um zu ihr zu gelangen, stelle man, analog dem Euclidischen Algorithmus, folgendes System von Gleichungen auf:

$$(66)\qquad \begin{array}{ll} gr = a_1 n + r_1, & 0 \overline{\gtrless} r_1 < n \\ gr_1 = a_2 n + r_2, & 0 \overline{\gtrless} r_2 < n \\ \ldots\ldots\ldots\ldots & \\ gr_i = a_{i+1} n + r_{i+1}, & 0 \overline{\gtrless} r_{i+1} < n \\ \ldots\ldots\ldots\ldots & ; \end{array}$$

aus den für die Reste r_i festgesetzten Grenzen folgen offenbar dann für jede der ganzen Zahlen a_i die Ungleichheiten $0 \overline{\gtrless} a_i < g$. Fafst man die Gleichungen (66) als Kongruenzen (mod. n) auf, so ergiebt sich aus ihnen

$$(67)\qquad gr_{i-1} \equiv r_i \pmod{n}$$

und daher allgemeiner

$$(68)\qquad g^m r_{i-1} \equiv r_{m+i-1} \pmod{n},$$

eine Kongruenz, welche für $i = 1$ die andere:

$$(69)\qquad g^m r \equiv r_m \pmod{n}$$

ergiebt.

Nun bricht die Reihe der Gleichungen dann und nur dann ab, wenn einer der Reste r_i Null wird; dies geschieht aber nach (69) für den Rest r_m dann und nur dann, wenn $g^m \cdot r \equiv 0$ (mod. n) d. h., weil r prim gegen n ist, wenn g^m teilbar ist durch n, was wieder nur dann geschehen kann, wenn n keine anderen Primfaktoren enthält, als sie g besitzt, alsdann aber für einen gewissen kleinsten Wert $m = h$ auch wirklich geschieht. In der That, ist

$$g = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}, \quad n = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k},$$

wo jedes α_i eine positive ganze Zahl, jedes β_i eine positive ganze Zahl oder Null bedeutet, so wird g^h durch n teilbar und die niedrigste Potenz von g sein, welche es ist, wenn h die kleinste ganze Zahl bezeichnet, für welche jedes $h\alpha_i \overline{\gtrless} \beta_i$, welche also gleich oder gröfser ist als jeder der Brüche $\frac{\beta_i}{\alpha_i}$. Ist insbesondere g aus lauter verschiedenen Primfaktoren zusammengesetzt, so wird h ganz

einfach dem gröfsten der Exponenten $\beta_1, \beta_2, \ldots \beta_k$ gleich zu setzen sein. Man findet zunächst folgendes Resultat:

Enthält n keine anderen Primfaktoren, als die Zahl g besitzt, so ist der Algorithmus (66) endlich und besteht, unter h die eben bezeichnete ganze Zahl verstanden, aus den h Gleichungen:

$$(70)\qquad \begin{aligned} gr &= a_1 n + r_1 \\ gr_1 &= a_2 n + r_2 \\ &\cdots\cdots \\ gr_{h-2} &= a_{h-1} n + r_{h-1} \\ gr_{h-1} &= a_h n, \end{aligned}$$

in jedem andern Falle läuft er ins Unendliche fort.

Aber man kann ihn auch in dem erstern Falle durch einen unendlichen Algorithmus ersetzen, indem man die letzte der Gleichungen (70) in der Form:

$$gr_{h-1} = (a_h - 1)n + r_h, \ (r_h = n)$$

schreibt und nun fortfährt, wie folgt:

$$(71)\qquad \begin{aligned} gr_h &= (g-1)n + r_{h+1}, \ (r_{h+1} = n) \\ gr_{h+1} &= (g-1)n + r_{h+2}, \ (r_{h+2} = n) \\ &\cdots\cdots\cdots \end{aligned}$$

Alsdann führt der Algorithmus in beiden Fällen, wie grofs die Zahl i auch gedacht werde, zur folgenden Formel:

$$(72)\qquad \frac{r}{n} = \frac{a_1}{g} + \frac{a_2}{g^2} + \frac{a_3}{g^3} + \cdots + \frac{a_i}{g^i} + \frac{r_i}{g^i n},$$

wenn man hier nur in dem zuvor betrachteten Falle, so oft $i > h - 1$ ist, a_h durch $a_h - 1$ und jede der folgenden Gröfsen $a_{h+1}, a_{h+2}, \ldots$ durch $g - 1$ ersetzt. Da nun $\frac{r_i}{g^i n} \overline{\gtrless} \frac{1}{g^i}$ ist, also mit unendlich wachsendem i gegen Null konvergiert, erschliefst man aus (72) diese konvergente Entwicklung für den reduzierten echten Bruch $\frac{r}{n}$:

$$(73)\qquad \frac{r}{n} = \frac{a_1}{g} + \frac{a_2}{g^2} + \frac{a_3}{g^3} + \frac{a_4}{g^4} + \cdots$$

oder den Satz: Jeder irreduktible echte Bruch $\frac{r}{n}$ läfst sich in einen unendlichen Ausdruck von der Gestalt (73) entwickeln, in welchem die Koeffizienten a_i, welche wir „die Ziffern“ der Entwicklung nennen wollen, positive ganze Zahlen $< g$ oder Null sind.

Zudem ist diese Entwicklung von $\frac{r}{n}$ in einen **unendlichen** Ausdruck von der Form (73) eindeutig. Gäbe es nämlich noch eine zweite unendliche Entwicklung dieser Art:

$$\frac{r}{n} = \frac{b_1}{g} + \frac{b_2}{g^2} + \frac{b_3}{g^3} + \frac{b_4}{g^4} + \cdots, \tag{74}$$

so sei a_m, b_m das erste Paar korrespondierender Ziffern, die von einander verschieden sind, sodafs eine derselben, etwa a_m, gröfser als die andere b_m sein und aus der Vergleichung von (73) und (74) die Gleichung

$$0 = \frac{a_m - b_m}{g^m} + \frac{a_{m+1} - b_{m+1}}{g^{m+1}} + \frac{a_{m+2} - b_{m+2}}{g^{m+2}} + \cdots$$

hervorgehen würde. In der letzteren ist das erste Glied $\overline{\gtrless} \frac{1}{g^m}$, offenbar aber die Gesamtheit aller folgenden Glieder algebraisch gröfser als

$$-\frac{g-1}{g^{m+1}} - \frac{g-1}{g^{m+2}} - \cdots = \frac{-1}{g^m},$$

die ganze rechte Seite der Gleichung, welche Null sein soll, wäre also algebraisch gröfser als Null, ein Widerspruch, aus welchem die Unzulässigkeit der Annahme hervorgeht.

Wenn für die bisher beliebig gedachte Grundzahl g die Zahl 10 gewählt wird, so ist ersichtlich die Entwicklung (73) nichts anderes als der Dezimalbruch für $\frac{r}{n}$ und der vorige Satz besagt daher im Besonderen: dafs jeder irreduktible echte Bruch auf eindeutige Weise in einen unendlichen Dezimalbruch sich entwickeln läfst von der Gestalt:

$$0, a_1 a_2 a_3 a_4 \ldots .$$

Aus (73) folgt weiter

$$g^i \cdot \frac{r}{n} = (a_1 g^{i-1} + a_2 g^{i-2} + \cdots + a_i) + \left(\frac{a_{i+1}}{g} + \frac{a_{i+2}}{g^2} + \cdots\right),$$

wo die zweite Klammer, weil kleiner als

$$(g-1)\left(\frac{1}{g} + \frac{1}{g^2} + \cdots\right) = 1,$$

ein echter Bruch sein mufs. Nun ist wegen $g^i r \equiv r_i \pmod{n}$ auch $g^i \cdot \frac{r}{n} = z + \frac{r_i}{n}$, wo z ganz und $\frac{r_i}{n}$ ein echter Bruch ist; folglich schliefst man die für jeden Wert des Index i giltige Formel:

$$\frac{r_i}{n} = \frac{a_{i+1}}{g} + \frac{a_{i+2}}{g^2} + \frac{a_{i+3}}{g^3} + \cdots \tag{75}$$

13. Wir zeigen nun weiter, dafs in der Entwicklung (73) des reduzierten Bruches $\frac{r}{n}$ die Folge der Ziffern

$$a_1, a_2, a_3, a_4, \ldots$$

periodisch ist. Die in dem unendlichen Algorithmus (66) resp. (70), (71) auftretenden unendlich vielen Zahlen $r, r_1, r_2, r_3, \ldots$ können nämlich, weil sie sämtlich nicht gröfser als n sind, nicht alle von einander verschieden sein. Sei daher r_h die erste von ihnen, welche einer späteren gleich wird, und unter diesen späteren sei r_{h+k} die erste, der sie gleich wird, derart, dafs h, k die kleinsten Zahlen sind, die erstere positiv oder Null, die zweite positiv, für welche

$$r_{h+k} = r_h \tag{76}$$

wird. Dann folgt aus den Kongruenzen

$$r_{h+1} \equiv g r_h, \quad r_{h+k+1} \equiv g r_{h+k},$$

dafs auch $r_{h+k+1} = r_{h+1}$, ebenso dann, dafs $r_{h+k+2} = r_{h+2}, \ldots r_{h+2k-1} = r_{h+k-1}$, endlich, dafs $r_{h+2k} = r_{h+k} = r_h$ ist, u. s. w. Die Reihe der Reste

$$r_h, r_{h+1}, \ldots r_{h+k-1}$$

und daher nach (66) die Reihe der Ziffern

$$a_{h+1}, a_{h+2}, \ldots a_{h+k} \tag{77}$$

wiederholt sich also ohne Ende und die ganze Reihe der Ziffern besteht aus h Anfangsgliedern

$$a_1, a_2, a_3, \ldots a_h \tag{78}$$

und der unaufhörlich wiederholten Periode (77) von k Gliedern. Die Zahlen h, k bestimmen sich hierbei folgendermafsen: Aus (76) folgt mit Rücksicht auf (69)

$$g^{h+k} \cdot r \equiv g^h \cdot r \pmod{n}$$

d. h., weil r prim ist gegen n,

$$g^h \cdot (g^k - 1) \equiv 0 \pmod{n}; \tag{79}$$

da nun auch umgekehrt aus dieser Kongruenz die Gleichheit (76) wieder hervorgeht, so sind h, k die kleinsten Zahlen, die erstere positiv oder Null, die zweite positiv, für welche diese Kongruenz erfüllt wird.

Man sieht aber auch leicht, dafs die Reihe der Ziffern keine andere (kleinste) Periode besitzt, als die eben bestimmte. Denn, bestände sie aus den i Anfangsgliedern

$$a_1, a_2, \ldots a_i$$

und einer stets wiederholten (kleinsten) Periode

$$a_{i+1}, a_{i+2}, \ldots a_{i+j},$$

so fände sich nach der Formel (75)

$$\frac{r_i}{n} = \frac{a_{i+1}}{g} + \frac{a_{i+2}}{g^2} + \cdots$$

$$\frac{r_{i+j}}{n} = \frac{a_{i+j+1}}{g} + \frac{a_{i+j+2}}{g^2} + \cdots$$

$$= \frac{a_{i+1}}{g} + \frac{a_{i+2}}{g^2} + \cdots$$

also $r_{i+j} = r_i$, was nach der Bedeutung der Zahlen h, k die Gleichheiten $i = h,\ j = k$ nach sich zieht.

Endlich kann man zeigen, dafs auch umgekehrt jede periodische Entwicklung von der Art (73) einen rationalen Bruch darstellt, der freilich nicht reduziert zu sein braucht. Gesetzt nämlich, die Reihe der Ziffern bestände aus h Anfangsgliedern und einer darauf folgenden Periode von k Gliedern, so folgt aus (73), indem man den unendlichen Ausdruck zur Rechten mit S bezeichnet,

$$S \cdot g^h = a_1 g^{h-1} + a_2 g^{h-2} + \cdots + a_h$$
$$+ \frac{a_{h+1}}{g} + \frac{a_{h+2}}{g^2} + \cdots$$

d. i., wenn das Polynom in der ersten Linie, das ganzzahligen Werth hat, z_h genannt wird,

$$S \cdot g^h = z_h + \frac{a_{h+1}}{g} + \frac{a_{h+2}}{g^2} + \cdots$$

und ebenso

$$S \cdot g^{h+k} = z_{h+k} + \frac{a_{h+k+1}}{g} + \frac{a_{h+k+2}}{g^2} + \cdots,$$

hieraus aber wegen der vorausgesetzten Periodizität der Ziffern durch Subtraktion beider Formeln

$$S \cdot g^h(g^k - 1) = z_{h+k} - z_h$$

also

$$S = \frac{z_{h+k} - z_h}{g^h\,(g^k - 1)}$$

d. h. gleich einem rationalen Bruche, der in seiner reduzierten Form $\frac{r}{n}$ nur einen Teiler von $g^h(g^k - 1)$ zum Nenner haben kann. —

Um nun die Periodizität der Entwicklung (73) näher zu untersuchen, denke man sich allgemein n in zwei Faktoren n_1, n_2 zerlegt, von denen der zweite prim gegen g, der erste nur aus solchen Primfaktoren zusammengesetzt ist, welche auch in g aufgehen, eine Zerlegung, wie sie immer möglich ist, wenn man für n_1, n_2 auch den Wert 1 zuläfst. Die kleinsten Zahlen h, k, welche die Kongruenz (79) erfüllen, sind dann offenbar die kleinsten Zahlen h, k, für welche

(80) g^h durch n_1, $g^k - 1$ durch n_2

teilbar ist.

Enthält mithin n sowohl Primteiler von g als auch solche, die nicht in g aufgehen, so ist die Entwicklung (73) stets gemischt periodisch, d. h. es ist vor der Periode noch ein anfänglicher Teil vorhanden; denn in diesem Falle sind n_1, n_2 beide von 1, also h von Null verschieden.

Enthält n nur Primteiler von g, so ist $n_2 = 1$ also $k = 1$, die unendliche Entwicklung (73) wäre also wieder gemischt periodisch, enthielte h anfängliche Glieder und eine eingliedrige Periode. Dies stimmt mit dem, was für diesen Fall in vor. Nr. schon gefunden worden ist, völlig überein, wo sich zudem aber noch gezeigt hat, dafs die Ziffer der Periode gleich $g - 1$ ist.

Ist endlich n prim gegen g, so ist $n_1 = 1$, $n_2 = n$ also $h = 0$ und k der Exponent, zu welchem g (mod. n) gehört. In diesem Falle ist also die Entwicklung (73) rein periodisch und die Anzahl der Ziffern in der Periode gleich dem Exponenten, zu welchem g (mod. n) gehört.

14. Für die Entwicklung rationaler Brüche in Dezimalbrüche d. h. bei der Annahme $g = 10 = 2 \cdot 5$, bei welcher g aus lauter verschiedenen Primfaktoren besteht, ergeben sich hieraus und aus dem, was für die Bestimmung der Zahl h in Nr. 12 gesagt worden ist, die folgenden (schon von Gaufs, *D. A. art.* 312—318 angegebenen) Sätze:

Ist $n = 2^\alpha 5^\beta \nu$, wo ν prim gegen 10, so ist der Dezimalbruch für $\frac{r}{n}$ endlich, wenn $\nu = 1$ ist, und er besteht alsdann aus α oder β Ziffern, jenachdem $\alpha > \beta$ oder $\beta > \alpha$ ist; er ist, wenn $\nu > 1$ ist, unendlich und besteht aus einem anfänglichen Teile von h Ziffern und einer Periode von k Ziffern, wo h die gröfsere der Zahlen α, β und k der Exponent ist, zu welchem 10 (mod. ν) gehört; mithin ist er dann gemischt periodisch, sobald n durch mindestens eine der Zahlen 2, 5 aufgeht, dagegen ist er rein periodisch und die Anzahl der Ziffern in der Periode dem Exponenten gleich, zu welchem 10 (mod. n) gehört, wenn n prim ist gegen 10.

Z. B. finden sich folgende Dezimalbrüche, welche die ausgesprochenen Sätze bestätigen:

1) $n = 80 = 2^4 \cdot 5$, $\alpha = 4$, $\beta = 1$, $h = 4$; $\frac{13}{80} = 0{,}1625$.

2) $n = 280 = 2^3 \cdot 5 \cdot 7$, $\alpha = 3$, $\beta = 1$, $h = 3$, $k = 6$, da $10^6 \equiv 1$ (mod. 7),

$$\frac{271}{280} = 0{,}967\,\overline{857142}\ldots$$

3) $n = 77 = 7 \cdot 11$; da $10^6 \equiv 1 \pmod{7}$, $10^2 \equiv 1 \pmod{11}$, so ist $10^6 \equiv 1 \pmod{77}$ und $k = 6$; so findet sich z. B.

$$\frac{23}{77} = 0{,}\overline{298701}\ldots.$$

Zur einfacheren Bildung solcher Dezimalbrüche im Falle grofser Nenner empfiehlt sich die Zerlegung des zu entwickelnden Bruches $\frac{r}{n}$ in Partialbrüche.

Sei allgemein

$$n = 2^\alpha 5^\beta p'^{\alpha'} p''^{\alpha''} \ldots,$$

wo $p', p'', \ldots$ von 2 und 5 verschiedene Primfaktoren, α, β positive ganze Zahlen oder Null, $\alpha', \alpha'' \ldots$ aber positive ganze Zahlen bedeuten. Dann läfst sich nach Kap. 4, Nr. 6 der irreduktible Bruch $\frac{r}{n}$ in eine Summe irreduktibler echter Brüche zerlegen, deren Nenner die einzelnen Primzahlpotenzen von n sind, nämlich

$$\frac{r}{n} = \frac{\varrho}{2^\alpha} + \frac{\sigma}{5^\beta} + \frac{r'}{p'^{\alpha'}} + \frac{r''}{p''^{\alpha''}} + \cdots + z,$$

wo z eine ganze Zahl ist, übrigens der erste bezw. zweite Bruch ausfällt, wenn α resp. β gleich Null ist. Denkt man sich nun die einzelnen Brüche zur Rechten in Dezimalbrüche entwickelt, so sind die Dezimalbrüche vom dritten an rein periodisch; heifsen $k', k'' \ldots$ die Ziffernanzahlen ihrer Perioden, so bedeuten diese Zahlen die Exponenten, zu denen 10 (mod. $p'^{\alpha'}$), (mod. $p''^{\alpha''}$), ... gehört, der Exponent k, zu welchem 10 (mod. $p'^{\alpha'} p''^{\alpha''} \ldots$) gehört, ist dann ihr kleinstes gemeinsames Vielfaches, sodafs, wenn $k = h'k' = h''k'' \ldots$ gesetzt wird, h' Perioden des ersten Dezimalbruchs aus genau soviel Ziffern bestehen, wie h'' Perioden des zweiten Dezimalbruchs u. s. w. Bei der Addition dieser Dezimalbrüche bildet sich daher offenbar eine Periode von k Ziffern. Der Dezimalbruch für $\frac{\varrho}{2^\alpha}$ aber, falls er vorhanden, ist endlich und besteht aus α, derjenige für $\frac{\sigma}{5^\beta}$ desgleichen und besteht aus β Ziffern; bedeutet h wieder die gröfsere der Zahlen α, β, so wird bei der Aufeinanderlegung der einzelnen Dezimalbrüche zur Bildung des Dezimalbruchs für $\frac{r}{n}$ die vorher gewonnene reine Periodizität gestört, man erhält einen anfänglichen Teil von h Ziffern, auf welchen eine Periode von k Ziffern folgt, ganz wie der obige allgemeine Satz es ausgesagt hat.

Z. B. sei gegeben der Bruch $\frac{513}{3080}$, dessen Nenner gleich $2^3 \cdot 5 \cdot 7 \cdot 11$ ist. Die a. a. O. gegebene Methode liefert zunächst folgende Partialbruchzerlegung

$$\frac{513}{3080} = \frac{1}{8} + \frac{3}{5} + \frac{5}{7} + \frac{8}{11} - 2.$$

Nun ist aber

$$\frac{1}{8} = 0,125$$

$$\frac{3}{5} = 0,6$$

$$\frac{5}{7} = 0,\overline{714285}\,\overline{714285}\ldots$$

$$\frac{8}{11} = 0,\overline{72}\,\overline{72}\,\overline{72}\,\overline{72}\,\overline{72}\,\overline{72}\ldots$$

$$-2 = -2$$

also

$$\frac{513}{3080} = 0,166\overline{558441}\ldots,$$

wie es die direkte Berechnung bestätigt.

15. Wir verfolgen nun den Fall noch weiter, wo n prim gegen g ist, in welchem die Entwicklung (73) rein periodisch, nämlich

$$\frac{r}{n} = \frac{a_1}{g} + \frac{a_2}{g^2} + \cdots + \frac{a_k}{g^k} + \frac{a_1}{g^{k+1}} + \frac{a_2}{g^{k+2}} + \cdots \tag{81}$$

ist; k bezeichnet den Exponenten, zu welchem g (mod. n) gehört. Nach (75) ist dann allgemein für jeden Wert des Index $i \gtreqless k$

$$\frac{r_i}{n} = \frac{a_{i+1}}{g} + \cdots + \frac{a_k}{g^{k-i}} + \frac{a_1}{g^{k-i+1}} + \cdots + \frac{a_i}{g^k} + \frac{a_{i+1}}{g^{k+1}} + \cdots \tag{82}$$

d. h. die Entwicklung von $\frac{r_i}{n}$ hat die gleiche, nur um i Stellen cyklisch verschobene Ziffernperiode wie diejenige von $\frac{r}{n}\cdot$ Zudem erkennt man aus dem Algorithmus (66), dafs, weil nach der Voraussetzung sowohl r als g und daher auch gr prim ist gegen n, dasselbe auch für r_1, demnach auch für r_2 u. s. w., allgemein für jeden Rest r_i gelten mufs. Die k Brüche (82) sind folglich sämtlich irreduktibel und, da die Zahlen $r_1, r_2, \ldots r_k$ verschieden von einander sind, gleichfalls verschieden.

In dem besonderen Falle, in welchem g primitive Wurzel von n, mithin $k = \varphi(n)$ ist, müssen die Zahlen $r_1, r_2, \ldots r_k$ mit den zu n primen Zahlen $< n$ identisch sein und somit der Ausdruck $\frac{r_i}{n}$ die sämtlichen $\varphi(n)$ irreduktiblen echten Brüche mit dem Nenner n darstellen. Der Formel (82) zufolge entstehen die Entwicklungen der letztern sämtlich aus der Entwicklung eines beliebigen von ihnen, wenn man dessen aus $\varphi(n)$ Ziffern bestehende Periode zu wiederholten Malen cyklisch permutiert. Wählt man z. B. $r = 1$ und setzt $r_i = \nu$, mithin zufolge (69) $i = \text{ind.}\,\nu$, so erhält man die Entwicklung

für $\frac{\nu}{n}$ aus derjenigen für $\frac{1}{n}$, wenn man die Periode der letzteren um soviel Stellen, als der ind. ν beträgt, cyklisch verschiebt.

So ist 10 primitive Wurzel (mod. 7) und

$$\frac{1}{7} = 0,\overline{142857}\ldots;$$

um hieraus den Dezimalbruch für $\frac{5}{7}$ zu erhalten, bedenke man, dafs $5 \equiv 10^5$ (mod. 7) oder ind. $5 = 5$ ist, dann ergiebt sich nach der vorigen Regel sofort

$$\frac{5}{7} = 0,\overline{714285}\ldots.$$

Ferner erhält man aus (82) die folgende Formel:

$$g^k \cdot \frac{r_i}{n} = a_{i+1} g^{k-1} + a_{i+2} g^{k-2} + \cdots + a_i + \frac{r_i}{n}$$

oder

$$\frac{g^k - 1}{n} \cdot r_i = a_{i+1} g^{k-1} + a_{i+2} g^{k-2} + \cdots + a_i,$$

und in gleicher Weise aus (81) diese andere:

$$\frac{g^k - 1}{n} \cdot r = a_1 g^{k-1} + a_2 g^{k-2} + \cdots + a_k,$$

sodafs die Beziehung

$$r_i(a_1 g^{k-1} + a_2 g^{k-2} + \cdots + a_k) = r(a_{i+1} g^{k-1} + a_{i+2} g^{k-2} + \cdots + a_i)$$

hervorgeht. Wenn nun wieder g als primitive Wurzel (mod. n) vorausgesetzt wird, so bedeutet r_i jede der zu n primen Zahlen $< n$; wählt man alsdann $r = 1$ und setzt $r_i = \nu$, mithin $i = \text{ind.}\,\nu$, so läfst die erhaltene Beziehung folgende Deutung zu: Sei N die ganze Zahl $\frac{g^{\varphi(n)} - 1}{n}$ und, in dem Systeme mit der Grundzahl g dargestellt,

$$N = a_1 g^{\varphi(n)-1} + a_2 g^{\varphi(n)-2} + \cdots + a_{\varphi(n)};$$

dann erhält man die Darstellung irgend eines Vielfachen νN in demselben Systeme, indem man einfach die Ziffern der ersteren Zahl um soviel Stellen cyklisch verschiebt, als der Index von ν beträgt. Dieser Satz ist vom Verfasser (*Ztschr. f. Math. u. Phys.* 36, 1891, p. 381) für den einfachsten Fall einer Primzahl n durch andere Betrachtung bewiesen, demnächst aber von J. Kraus (ebendas. 37, 1892, p. 190) aus den hier benutzten Prinzipien hergeleitet worden.

Als Beispiel diene der Fall $g = 10$, $n = 7$, in welchem

$$N = \frac{10^6 - 1}{7} = 142857, \quad \text{ind.}\,1 = 0,$$

$$2N = 285714, \quad \text{ind.}\,2 = 2,$$

$$3N = 428571, \quad \text{ind. } 3 = 1,$$
$$4N = 571428, \quad \text{ind. } 4 = 4,$$
$$5N = 714285, \quad \text{ind. } 5 = 5,$$
$$6N = 857142, \quad \text{ind. } 6 = 3$$

ist. Vergleicht man diese Vielfachen von N mit den ihnen beigefügten Indices ihrer Multiplikatoren, so sieht man durch sie den ausgesprochenen Satz vollkommen bestätigt.

16. Schon gelegentlich der Darstellung ganzer Zahlen in einem gegebenen Ziffernsysteme ist von der Veränderung gehandelt worden, welche die Ziffern erleiden, wenn statt der Grundzahl des Systems irgend eine andere gewählt wird. Das Gleiche gilt für die Darstellung rationaler Brüche $\frac{r}{n}$ in der Form (73), die nur eine Fortsetzung jener früheren Darstellung ist. Wird nämlich statt der Grundzahl g eine andere g' gewählt, so erhält man an Stelle des Algorithmus (66) den folgenden:

$$g'r = a_1'n + r_1', \quad 0 \overline{\gtrless} r_1' < n,$$
$$g'r_1' = a_2'n + r_2', \quad 0 \overline{\gtrless} r_2' < n,$$
$$g'r_2' = a_3'n + r_3', \quad 0 \overline{\gtrless} r_3' < n,$$
$$\cdots\cdots\cdots\cdots\cdots$$

aus welchem u. a. die der Kongruenz (69) entsprechende Kongruenz

$$g'^m \cdot r \equiv r_m' \pmod{n} \tag{83}$$

sowie die neue Entwicklung

$$\frac{r}{n} = \frac{a_1'}{g'} + \frac{a_2'}{g'^2} + \frac{a_3'}{g'^3} + \cdots \tag{84}$$

hervorgeht. Wird hierbei g' wie g als relativ prim zu n vorausgesetzt, so ist auch diese Entwicklung, wie die Entwicklung (73), rein periodisch und die Ziffernanzahl der Periode wird für beide Entwicklungen die gleiche sein, falls außerdem g, g' zu demselben Exponenten (mod. n) gehören. Letzteres ist der Fall, sooft g, g' (mod. n) kongruent oder associiert sind, zwei Fälle, für welche wir nun den Zusammenhang zwischen den Ziffern beider Entwicklungen noch feststellen wollen.

Sei zuerst $g' \equiv g \pmod{n}$ oder $g' = g + hn$. Dann ist auch

$$g'r \equiv gr \quad \text{d. h.} \quad a_1'n + r_1' \equiv a_1n + r_1 \pmod{n}$$

folglich $r_1' = r_1$; deshalb ist

$$g'r_1' \equiv gr_1 \quad \text{d. h.} \quad a_2'n + r_2' \equiv a_2n + r_2 \pmod{n}$$

also auch $r_2' = r_2$, nunmehr auch $r_3' = r_3$ u. s. f., allgemein $r_i' = r_i$. Daher folgen aus den beiden allgemeinen Gleichungen der Algorithmen:

$$(85) \qquad g' r_i' = a_{i+1}' n + r_{i+1}', \qquad g r_i = a_{i+1} n + r_{i+1}$$

die folgenden für jeden Wert des Index i giltigen:

$$(86) \quad (a_{i+1}' - a_{i+1}) n = (g' - g) r_i, \quad (g a_{i+1}' - g' a_{i+1}) n = (g' - g) r_{i+1}$$

oder, wenn in der letzteren $i-1$ statt i gesetzt und dann die erstere berücksichtigt wird, für $i > 0$:

$$(g a_i' - g' a_i) n = (a_{i+1}' - a_{i+1}) n,$$

mithin erhält man zwischen den Ziffern der beiden Entwicklungen des Bruches $\frac{r}{n}$ folgende, für jeden Wert des Index $i > 0$ bestehende Relation:

$$(87) \qquad g a_i' + a_{i+1} = g' a_i + a_{i+1}';$$

sie giebt sämtliche Ziffern a_i' mit Ausnahme von a_1' mittels der Ziffern a_i, zur Bestimmung von a_1' aber findet sich leicht $a_1' = a_1 + hr$.

Sei zweitens $gg' \equiv 1 \pmod{n}$. Dann ist der Formel (83) entsprechend

$$g'^i \cdot r \equiv r_i' \pmod{n}.$$

Da aber $g' \equiv g^{k-1}$ ist, wenn wieder k der Exponent ist, zu welchem $g \pmod{n}$ gehört, so nimmt die voraufgehende Kongruenz die Form an:

$$g^{(k-1)i} \cdot r \equiv r_i' \pmod{n}$$

und, da nach (69) und mit Rücksicht auf (76), falls $i < k$ ist, auch

$$g^{(k-1)i} \cdot r \equiv r_{(k-1)i} \equiv r_{k-i}$$

gesetzt werden kann, so ergiebt sich die Beziehung

$$(88) \qquad r_i' = r_{k-i} \qquad (i < k).$$

Nunmehr setze man in der zweiten der Gleichungen (85), die auch hier dem Algorithmus zum Grunde liegen, $k-i$ statt i, was voraussetzt, dafs $i \overline{<} k$ sei, sodafs sie die Form annimmt

$$(89) \qquad g r_{k-i} = a_{k-i+1} \cdot n + r_{k-i+1};$$

dann ergiebt sich wegen (88) aus ihrer Verbindung mit der ersten jener Gleichungen die nachstehende:

$$0 = (g a_{i+1}' - g' a_{k-i+1}) n + g r_{i+1}' - g' r_{k-i+1}$$

und, wenn die erste der Gleichungen (85), nachdem darin $i-1$ statt i gesetzt, von der Gleichung (89), nachdem in dieser $i+1$ statt i gesetzt worden, was $i < k-1$ voraussetzt, subtrahiert wird, die folgende:

$$g r_{k-i-1} - g' r_{i-1}' = (a_{k-i} - a_i') n;$$

aus der Addition dieser beiden aber entsteht, da nach (88) $r_{i+1}' = r_{k-i-1}$, $r_{i-1}' = r_{k-i+1}$ ist, diese andere:

$$0 = (g a_{i+1}' - g' a_{k-i+1}) n + (a_{k-i} - a_i') n$$

d. h. man erhält in diesem Falle zwischen den Ziffern der beiden Entwicklungen von $\frac{r}{n}$ für jeden von 0 verschiedenen Wert des Index $i < k - 1$ die Relation:

$$ga'_{i+1} + a_{k-i} = g'a_{k-i+1} + a'_i. \tag{90}$$

Wird endlich die erste Gleichung des ersten Algorithmus:

$$gr = a_1 n + r_1$$

mit g' multipliziert und die Gleichung

$$g' r'_{k-1} = a'_k n + r'_k$$

sowie die Gleichheiten $r_1 = r'_{k-1}$, $r'_k = r$ berücksichtigt, so findet sich ohne Mühe noch die folgende Beziehung:

$$\frac{gg' - 1}{n} \cdot r = g' a_1 + a'_k$$

und auf analoge Weise diese andere:

$$\frac{gg' - 1}{n} \cdot r = g a'_1 + a_k,$$

welche ergänzend zur allgemeinen Relation (90) hinzutreten, um alle Ziffern der zweiten Entwicklung auf diejenigen der ersteren zurückzuführen.

Auch diese Resultate, auf welche bereits in Kap. 2, Nr. 11 hingewiesen wurde, sind zuerst von J. Kraus in einer dort angeführten Arbeit bewiesen.

17. Von den binomischen Kongruenzen, die im Vorigen ausschliefslich betrachtet worden sind, wenden wir uns nunmehr zu den allgemeinen Kongruenzen eines beliebigen Grades*) d. i. den Kongruenzen von der Form

$$f(x) \equiv 0 \pmod{n}, \tag{91}$$

*) Die Theorie der höheren Kongruenzen ist in ihren wesentlichsten Teilen bereits von Gaufs erledigt worden, doch hat er selbst von seinen bezüglichen Untersuchungen nichts veröffentlicht; erst aus seinem Nachlasse ist eine fragmentarische Arbeit darüber herausgegeben worden (*Werke* II, p. 212). Nächst Galois, welcher durch Einführung eigentümlicher „Imaginären" (*Bull. de Férussac* 13, 1830, p. 398) die gedachte Theorie zu entwickeln wufste, hat als Erster Schönemann (*Journ. f. Math.* 31, 1846, p. 269 und 32, p. 93) eine ausführliche Darstellung derselben gegeben, demnächst Dedekind (ebend. 54, 1857, p. 1), welcher die seinige auf die gleichen Prinzipien gründete, auf denen die Theorie der Kongruenzen ganzer Zahlen beruht. J. A. Serret gab eine ähnliche Begründung der Theorie in Ausführung einer der Akad. d. Wissensch. zu Paris am 4. Dezbr. 1865 vorgelegten Abhandlung in seinem *Handbuch der höh. Algebra*, deutsch v. Wertheim, II, p. 96. Im Folgenden werden diese Arbeiten durch den Namen ihrer Verfasser zitiert werden.

in welcher $f(x)$ eine ganze, ganzzahlige Funktion von x und n eine beliebige (positive) ganze Zahl ist, welche, in Primfaktoren zerlegt,

$$(92) \qquad n = 2^\lambda p^\alpha p'^{\alpha'} \ldots$$

sei. Soll die Kongruenz (91) eine Wurzel haben, so mufs diese auch Wurzel einer jeden der Kongruenzen

$$(93) \quad f(x) \equiv 0 \text{ (mod. } 2^\lambda), \quad f(x) \equiv 0 \text{ (mod. } p^\alpha), \quad f(x) \equiv 0 \text{ (mod. } p'^{\alpha'}), \ldots$$

sein, und demnach wäre (91) unlösbar, wenn auch nur eine dieser abgeleiteten Kongruenzen unmöglich ist. Sind aber im Gegenteil diese letzteren sämtlich auflösbar, so ist es auch die Kongruenz (91) und alle ihre Wurzeln ergeben sich aus denjenigen der abgeleiteten Kongruenzen in der in Nr. 10 angegebenen Weise. Demnach kommt die Betrachtung der Kongruenz (91) auf die der einfacheren Kongruenzen (93) durchaus zurück und es ist nur nötig, sich mit den letzteren zu beschäftigen.

Wir behandeln hier aber nur den wichtigsten und zugleich einfachsten Fall, die Kongruenzen von der Form

$$(94) \qquad f(x) \equiv 0 \text{ (mod. } p),$$

wo p eine ungerade Primzahl ist*).

In einer solchen Kongruenz dürfen ohne Einflufs auf ihre etwaigen Wurzeln die Koeffizienten durch (mod. p) kongruente Zahlen ersetzt werden. Nennt man also zwei ganze Funktionen $f(x)$, $\varphi(x)$ (mod. p) kongruent, in Zeichen:

$$(95) \qquad f(x) \equiv \varphi(x) \text{ (mod. } p),$$

wenn die Koeffizienten gleich hoher Potenzen von x in ihnen (mod. p) kongruent sind, so darf die Kongruenz (94) durch jede der Kongruenzen

$$(96) \qquad \varphi(x) \equiv 0 \text{ (mod. } p)$$

ersetzt werden, in denen $\varphi(x)$ mit $f(x)$ kongruent ist (mod. p). Somit dürfen z. B. alle Glieder in $f(x)$ unterdrückt werden, deren Koeffizienten durch p teilbar sind. Wären dies sämtliche Koeffizienten, so bestünde die Kongruenz (94) identisch d. h. für jedes ganzzahlige x; im entgegengesetzten Falle giebt es ein höchstes Glied in $f(x)$, dessen Koeffizient durch p nicht teilbar ist; der Exponent m dieses Gliedes heifse der Grad der Kongruenz (94), welche alsdann durch diese:

$$(97) \qquad ax^m + a_1 x^{m-1} + \cdots + a_{m-1} x + a_m \equiv 0 \text{ (mod. } p)$$

ersetzt werden darf. Da a durch p nicht teilbar, so lassen sich

*) Einiges über den allgemeineren Fall, wo der Modulus eine Primzahlpotenz p^α, findet sich in der zweiten der zuvor zitierten Schönemannschen Arbeiten.

Zahlen $\alpha_1, \alpha_2, \ldots \alpha_m$ so bestimmen, dafs allgemein $a_i \equiv a\alpha_i \pmod{p}$ ist; demnach nimmt die Kongruenz (97) die Gestalt:

$$a(x^m + \alpha_1 x^{m-1} + \cdots + \alpha_{m-1} x + \alpha_m) \equiv 0$$

oder noch einfacher die folgende:

$$x^m + \alpha_1 x^{m-1} + \cdots + \alpha_{m-1} x + \alpha_m \equiv 0 \pmod{p} \tag{98}$$

an, in welcher der Koeffizient des höchsten Gliedes die Einheit ist. Diese Gestalt der Kongruenz heifst ihre primäre Form.

Der Grad eines Produktes $\varphi(x)\psi(x)$ ist die Summe der Grade seiner Faktoren. Denn, ist

$$\varphi(x) \equiv \alpha x^\mu + \cdots, \quad \psi(x) \equiv \beta x^\nu + \cdots \pmod{p},$$

wo α, β durch p nicht teilbar sind, so wird

$$\varphi(x)\psi(x) \equiv \alpha\beta \cdot x^{\mu+\nu} + \cdots \pmod{p},$$

wo auch $\alpha\beta$ durch p nicht aufgeht, mithin ist $\mu + \nu$ der Grad des Produktes.

Ist daher $\varphi(x)\psi(x) \equiv 0 \pmod{p}$ d. h. sind alle Koeffizienten eines Produktes teilbar durch p, so gilt dies auch von mindestens einem der Faktoren; denn sonst hätte $\varphi(x)$ einen bestimmten Grad μ (der auch gleich 0 sein könnte), $\psi(x)$ einen bestimmten Grad ν und deshalb auch das Produkt einen bestimmten Grad $\mu + \nu$, was der Annahme zuwider ist.

In Kap. 3, Nr. 4 ist bereits gezeigt, dafs die Kongruenz (97) nicht mehr als m Wurzeln haben kann. Ist aber $x \equiv \xi \pmod{p}$ eine Wurzel derselben, so ist

$$a\xi^m + a_1 \xi^{m-1} + \cdots + a_{m-1}\xi + a_m \equiv 0 \pmod{p}$$

und man darf daher, ohne die Lösungen der Kongruenz (97) zu beeinflussen, diesen Ausdruck von ihrer linken Seite abziehen, wodurch sie die Form

$$a(x^m - \xi^m) + a_1(x^{m-1} - \xi^{m-1}) + \cdots + a_{m-1}(x - \xi) \equiv 0$$

oder, da hier jedes Glied algebraisch durch $x - \xi$ teilbar ist, die folgende Gestalt:

$$(x - \xi) \cdot f_1(x) \equiv 0 \pmod{p}$$

erhält, in welcher $f_1(x)$ eine ganze Funktion mit ganzzahligen Koeffizienten bedeutet, deren höchster gleich a und deren Grad $m - 1$ ist. Hat demnach (94) eine ganzzahlige Lösung ξ, so zerfällt $f(x)$ nach der Formel

$$f(x) \equiv (x - \xi) f_1(x) \pmod{p} \tag{99}$$

in zwei Faktoren (mod. p), deren einer der Linearfaktor $x - \xi$, der andere eine ganze und ganzzahlige Funktion

$m-1^{\text{ten}}$ Grades ist. In diesem Falle ist also $f(x)$ eine (mod. p) reduktible Funktion.

Hieraus folgt nun zwar unmittelbar, daſs, wenn die Funktion $f(x)$ (mod. p) irreduktibel, nämlich eine Zerfällung derselben nach der Kongruenz

$$f(x) \equiv \varphi(x)\,\psi(x) \pmod{p} \tag{100}$$

in ganze, ganzzahlige Faktoren $\varphi(x)$, $\psi(x)$ nicht möglich ist, die Kongruenz (94) keine ganzzahligen Lösungen haben kann. Das Umgekehrte ist aber keineswegs notwendig der Fall, vielmehr kann die Kongruenz (94) in ganzen Zahlen unlösbar und gleichwohl $f(x)$ nach der Formel (100) in Faktoren zerlegbar sein. Die Auflösbarkeit der Kongruenz (94) entspricht nämlich dem besonderen Falle, daſs einer dieser Faktoren ein Linearfaktor ist.

So führt die Auflösung der Kongruenz (94) in ganzen Zahlen zu einer allgemeineren Aufgabe, mit deren Lösung sie zugleich geliefert wird, zu der Aufgabe: die Zerlegbarkeit der Funktion $f(x)$ in (mod. p) irreduktible Faktoren zu untersuchen. Mit solcher Zerlegung, welche auf ganz analogen Prinzipien beruht, wie die Zerfällung der ganzen Zahlen in Primfaktoren, werden wir nunmehr uns eingehend beschäftigen.

18. Alle ganzen und ganzzahligen Funktionen von x bilden in ihrer Gesamtheit einen sogenannten Modulus (s. Kap. 2, Nr. 2), insofern die Summe und die Differenz zweier solcher Funktionen wieder eine solche Funktion ist. Das Gleiche gilt aber offenbar auch von der Gesamtheit $\overline{M}$ aller derjenigen Funktionen, deren sämtliche Koeffizienten durch p teilbar, welche also das p-fache einer andern ganzzahligen Funktion oder, einer vorher eingeführten Bezeichnung gemäſs, kongruent Null (mod. p) sind. Die zuvor definierte Kongruenz

$$f(x) \equiv \varphi(x) \pmod{p} \tag{101}$$

zweier ganzen Funktionen in Bezug auf den Modulus p besagt offenbar nichts anderes, als daſs die Differenz $f(x)-\varphi(x)$ zu dieser Gesamtheit $\overline{M}$ gehört oder daſs eine Gleichung besteht von der Form

$$f(x) = \varphi(x) + p\cdot\psi(x), \tag{102}$$

wo auch $\psi(x)$ eine ganze, ganzzahlige Funktion von x ist. Offenbar sind daher zwei Funktionen, welche einer dritten (mod. p) kongruent sind, es auch unter einander, und die sämtlichen ganzen, ganzzahligen Funktionen verteilen sich in Klassen derart, daſs zwei Funktionen (mod. p) kongruent sind dann und nur dann, wenn sie zu der gleichen Klasse gehören. Die Anzahl dieser Klassen ist unendlich groſs, denn es giebt (mod. p) Funktionen von jedem beliebigen Grade, zwei Funktionen (mod. p) verschiedenen Grades aber können ersichtlich

nicht zu der gleichen Klasse gehören. Vergleicht man nun die unendliche Menge dieser Klassen derjenigen aller ganzen Zahlen, so spielen dagegen die Individuen ein- und derselben Klasse (mod. p) die Rolle einer einzigen Zahl, da sie offenbar in allen Kongruenzfragen in Bezug auf den Modulus p durch eine beliebig gewählte Funktion dieser Klasse, den Repräsentanten derselben, vertreten werden können.

Die Anzahl aller (mod. p) inkongruenten d. h. zu verschiedenen Klassen gehörigen Funktionen vom Grade m ist, wie leicht zu sehen, gleich $(p-1)p^m$. Denn alle diese Funktionen haben (mod. p) die Form

$$ax^m + a_1 x^{m-1} + \cdots + a_{m-1}x + a_m,$$

wo a nicht teilbar ist durch p, und da zwei solcher Funktionen (mod. p) einander kongruent oder nicht kongruent sind, jenachdem in ihnen sämtliche entsprechende Koeffizienten (mod. p) kongruent sind oder auch nur einmal zwei solche Koeffizienten nicht kongruent sind, so bildet man die sämtlichen inkongruenten Funktionen m^{ten} Grades, wenn man für a die Zahlen $1, 2, 3, \ldots p-1$, für jeden der anderen Koeffizienten aber die Zahlen $0, 1, 2, 3, \ldots p-1$ setzt, durch deren Kombination man in der That $(p-1)p^m$ Funktionen erhält. Da bei den primären Funktionen m^{ten} Grades der Koeffizient a nur den einen Wert 1 erhalten darf, beträgt insbesondere die Anzahl der (mod. p) inkongruenten **primären** Funktionen m^{ten} Grades nur p^m.

Besteht nun eine Kongruenz von der Form (100):

$$f(x) \equiv \varphi(x)\ \psi(x) \pmod{p},$$

so heifst jede der beiden ganzen ganzzahligen Funktionen $\varphi(x)$, $\psi(x)$ ein Faktor oder ein Divisor oder Teiler von $f(x)$ (mod. p); er kann offenbar durch irgend eine andere, der gleichen Klasse angehörige Funktion ersetzt werden, sodafs auch hierbei wieder alle Individuen derselben Klasse sich wie eine einzige Zahl verhalten. Der Grad eines Teilers ist niemals gröfser als derjenige der Funktion; denn, heifsen μ, ν die Grade von $\varphi(x)$, $\psi(x)$, so mufs der Grad m von $f(x)$ dem Grade $\mu + \nu$ der kongruenten Funktion $\varphi(x)\ \psi(x)$ gleich, $m = \mu + \nu$ sein.

Jede Funktion hat jede der Zahlen $1, 2, 3, \ldots p-1$ zu Teilern; denn, ist α eine dieser Zahlen und α' ihr Sozius, also $\alpha\alpha' \equiv 1 \pmod{p}$, so besteht die Kongruenz

$$f(x) \equiv \alpha\alpha' \cdot f(x) \equiv \alpha \cdot \psi_\alpha(x) \pmod{p},$$

wenn $\psi_\alpha(x) = \alpha' \cdot f(x)$ gedacht wird. Weil somit die genannten Zahlen (d. h. die (mod. p) inkongruenten Funktionen nullten Grades) sich verhalten, wie mit Bezug auf die Teilbarkeit ganzer Zahlen die

Eins, so sollen sie Einheiten (mod. p) genannt werden. Die durch die vorige Kongruenz für die verschiedenen Werte $\alpha = 1, 2, 3, \ldots p-1$ definierten Funktionen $\psi_\alpha(x)$ sollen als (mod. p) nicht wesentlich von $f(x)$ verschiedene Funktionen bezeichnet werden. Jede Funktion $f(x)$ hat also alle nicht wesentlich von ihr verschiedenen Funktionen zu Teilern. Besitzt aber eine Funktion aufser Einheiten keine wesentlich von ihr verschiedenen Teiler, so wird sie eine (mod. p) irreduktible Funktion oder eine Primfunktion (mod. p) genannt.

19. Wenn zwei Funktionen $f_1(x)$, $f_2(x)$ ein- und dieselbe Funktion $\varphi(x)$ zum Teiler (mod. p) haben, sodafs zwei Kongruenzen bestehen von der Form

$$f_1(x) \equiv \varphi(x)\,\psi_1(x), \quad f_2(x) \equiv \varphi(x)\,\psi_2(x) \pmod{p},$$

so heifst $\varphi(x)$ ein (mod. p) gemeinsamer Teiler von $f_1(x)$, $f_2(x)$. Zur Bestimmung aller dieser (mod. p) gemeinsamen Teiler besteht ein Algorithmus, der dem Euclidischen völlig analog ist. In der That läfst sich eine Kongruenz aufstellen von der Form:

$$f_1(x) \equiv f_2(x)\,q_1(x) + f_3(x) \pmod{p}, \tag{103}$$

worin $q_1(x)$, $f_3(x)$ ganze ganzzahlige Funktionen, die letztere von kleinerem Grade als $f_2(x)$ ist. Ist nämlich der Grad m_1 von $f_1(x)$ kleiner als der Grad m_2 von $f_2(x)$, so setze man, um (103) zu erfüllen, $q_1(x) = 0$, $f_3(x) = f_1(x)$; im entgegengesetzten Falle seien a_1, a_2 die Koeffizienten der höchsten Glieder in $f_1(x)$, $f_2(x)$ und $a_2\alpha_2 \equiv a_1$ (mod. p), dann fällt in $f_1(x) - \alpha_2 x^{m_1 - m_2} \cdot f_2(x)$ (mod. p) das höchste Glied aus und der Grad m_1' der Differenz ist höchstens $m_1 - 1$; behandelt man diese Differenz wieder ähnlich, so kommt man zu einem Ausdrucke

$$f_1(x) - \alpha_2 x^{m_1 - m_2} \cdot f_2(x) - \alpha_2' \cdot x^{m_1' - m_2} \cdot f_2(x),$$

dessen Grad wieder geringer ist, u. s. w., endlich zu einer Differenz

$$f_1(x) - q_1(x) f_2(x),$$

deren Grad (mod. p) kleiner ist als m_2; setzt man diese Funktion oder irgend eine ihr (mod. p) kongruente gleich $f_3(x)$, so wird die Kongruenz (103) erfüllt.

Nun kann man dieselbe Betrachtung, wie hier für die Funktionen $f_1(x)$, $f_2(x)$, auch anstellen für die beiden Funktionen $f_2(x)$, $f_3(x)$ und somit eine Kongruenz

$$f_2(x) \equiv f_3(x)\,q_2(x) + f_4(x) \pmod{p} \tag{103}$$

aufstellen, in welcher $f_4(x)$ von geringerem Grade ist als $f_3(x)$, u. s. w. So fortgehend mufs man endlich auf eine Funktion $f_k(x)$, welche (mod. p) kongruent Null ist, also auf eine Kongruenz von der Form

$$(103) \qquad f_{k-2}(x) \equiv f_{k-1}(x) \cdot q_{k-2}(x) \pmod{p}$$

geführt werden, denn sonst würde der bezeichnete Prozefs, der wegen der Abnahme der Grade von $f_1(x)$, $f_2(x)$, $f_3(x), \ldots$ nur endlich sein kann, unendlich weit fortlaufen. Durchgeht man dann die Reihe der mit (103) bezeichneten Kongruenzen in der aufgestellten Folge, so erkennt man leicht, dafs jeder (mod. p) gemeinsame Teiler von $f_1(x)$, $f_2(x)$ wegen der vorletzten Kongruenz

$$(103) \qquad f_{k-3}(x) \equiv f_{k-2}(x) \cdot q_{k-3}(x) + f_{k-1}(x) \pmod{p}$$

auch ein Teiler von $f_{k-1}(x)$ sein mufs; durchläuft man sie in der entgegengesetzten Richtung, so findet sich umgekehrt jeder Teiler von $f_{k-1}(x)$ (mod. p) auch als ein gemeinsamer Teiler von $f_1(x)$, $f_2(x)$, weshalb offenbar die (mod. p) gemeinsamen Teiler von $f_1(x)$, $f_2(x)$ identisch sind mit den sämtlichen (mod. p) vorhandenen Teilern der Funktion $f_{k-1}(x)$, die selbst ein solcher gemeinsamer Teiler und zwar, da die Teiler einer Funktion (mod. p) geringeren Grades sind als die Funktion selbst, der gemeinsame Teiler höchsten Grades ist. Dieser letztere gemeinsame Teiler heifse der gröfste gemeinsame Teiler von $f_1(x)$, $f_2(x)$.

Man übersieht ferner, ganz analog wie beim Euclidischen Algorithmus, dafs aus den Kongruenzen (103) sich eine andere Kongruenz ergiebt von folgender Form:

$$(104) \qquad f_1(x) \cdot \varphi_1(x) + f_2(x) \cdot \varphi_2(x) \equiv d(x) \pmod{p},$$

in welcher der bisher mit $f_{k-1}(x)$ bezeichnete gröfste gemeinsame Teiler von $f_1(x)$, $f_2(x)$ durch das Zeichen $d(x)$ ersetzt worden ist, $\varphi_1(x)$, $\varphi_2(x)$ aber gewisse ganze, ganzzahlige Funktionen bedeuten.

Ist der gröfste gemeinsame Teiler $d(x)$ zweier ganzen Funktionen $f_1(x)$, $f_2(x)$ eine Einheit e (mod. p), so werden diese Funktionen relativ prime Funktionen genannt. Die Gleichung (104) erhält alsdann die Gestalt

$$f_1(x) \cdot \varphi_1(x) + f_2(x) \cdot \varphi_2(x) \equiv e \pmod{p}$$

oder, indem man mit dem Sozius ε von e multipliziert und $\varepsilon\varphi_1(x) = \psi_1(x)$, $\varepsilon\varphi_2(x) = \psi_2(x)$ setzt, die Gestalt

$$(105) \qquad f_1(x) \cdot \psi_1(x) + f_2(x) \cdot \psi_2(x) \equiv 1 \pmod{p},$$

und somit ergiebt sich der Satz: Für relativ prime Funktionen $f_1(x)$, $f_2(x)$ hat die Kongruenz

$$(106) \qquad f_1(x) \cdot X_1 + f_2(x) \cdot X_2 \equiv 1 \pmod{p}$$

stets eine Auflösung, bei welcher X_1, X_2 ganze ganzzahlige Funktionen von x sind.

Aus diesen letzten Resultaten fliefsen nun die wichtigsten Folgerungen. Zunächst der Satz: Sind $f_1(x)$, $f_2(x)$ (mod. p) relativ

prime Funktionen, $\varphi(x)$ aber eine beliebige ganze, ganzzahlige Funktion, so ist jeder (mod. p) gemeinsame Teiler von $f_1(x)\cdot\varphi(x)$ und $f_2(x)$ auch ein (mod. p) gemeinsamer Teiler von $\varphi(x)$ und $f_2(x)$. Denn aus (105) folgt

$$f_1(x)\,\varphi(x)\cdot\psi_1(x)+f_2(x)\cdot\varphi(x)\,\psi_2(x)\equiv\varphi(x)\ (\text{mod.}\ p),$$

jeder gemeinsame Teiler von $f_1(x)\varphi(x)$ und $f_2(x)$ ist demnach auch (mod. p) ein Teiler von $\varphi(x)$, w. z. b. w.

Wenn also $f_1(x)\cdot\varphi(x)$ (mod. p) **teilbar** ist durch die zu $f_1(x)$ prime Funktion $f_2(x)$, so mufs $f_2(x)$ (mod. p) ein **Teiler** von $\varphi(x)$ sein.

Ist aber auch $\varphi(x)$ (mod. p) relativ prim zu $f_2(x)$, so können $f_1(x)\cdot\varphi(x)$ und $f_2(x)$ so wenig wie $\varphi(x)$ und $f_2(x)$ einen von einer Einheit verschiedenen Teiler gemeinsam haben, man findet daher den neuen Satz: Sind zwei (oder mehr) Funktionen (mod. p) relativ prim zu ein- und derselben Funktion, so ist es zu dieser auch ihr Produkt.

Bezeichnet nun $P(x)$ eine Primfunktion (mod. p), so hat diese nur die wesentlich verschiedenen Teiler 1 und $P(x)$. Gesetzt also, das Produkt $f(x)\cdot\varphi(x)$ sei (mod. p) teilbar durch $P(x)$, so sind nur folgende Fälle möglich: entweder hat $f(x)$ den Teiler $P(x)$ (mod. p); andernfalls kann $f(x)$ mit $P(x)$ nur eine Einheit zum (mod. p) gemeinsamen Teiler haben, dann ist es relativ prim zu $P(x)$ und nach dem vorletzten Satze folgt aus der Voraussetzung, dafs dann $\varphi(x)$ (mod. p) durch $P(x)$ teilbar ist. Somit erhält man den Satz: Ist ein Produkt von Funktionen (mod. p) durch eine Primfunktion teilbar, so ist es auch einer der Faktoren.

20. Auf Grund dieser Sätze ergiebt sich die eindeutige Zerlegbarkeit der ganzen Funktionen (mod. p) in Primfunktionen in ganz derselben Weise, wie diejenige der ganzen Zahlen in Primfaktoren. In der That: eine Funktion $f(x)$ ist entweder selbst Primfunktion oder besitzt einen oder mehrere wesentlich von $f(x)$ und einer Einheit verschiedene Teiler (mod. p), die geringeren Grades sind als $f(x)$ selbst. Ist $P^0(x)$ ein solcher geringsten Grades, so mufs $P^0(x)$ Primfunktion sein, denn jeder von $P^0(x)$ verschiedene Teiler von $P^0(x)$ wäre von geringerem Grade als $P^0(x)$ und offenbar auch (mod. p) ein Teiler von $f(x)$, gegen die Bedeutung von $P^0(x)$. Setzt man demgemäfs

$$f(x)\equiv P^0(x)\cdot f_1(x)\ (\text{mod.}\ p), \tag{107}$$

wo $f_1(x)$ eine ganze, ganzzahlige Funktion geringeren Grades (mod. p) wie $f(x)$ bedeutet, so kann man, falls nicht $f_1(x)$ selbst eine Primfunktion, also $f(x)$ nach der vorigen Kongruenz bereits in Primfunktionen zerlegt ist, für $f_1(x)$ eine analoge Kongruenz aufstellen:

$$f_1(x)\equiv P'(x)\cdot f_2(x)\ (\text{mod.}\ p), \tag{108}$$

in welcher $P'(x)$ eine Primfunktion bedeutet, die möglicherweise mit $P^0(x)$ identisch ist, $f_2(x)$ aber eine neue ganze, ganzzahlige Funktion ist, welche wieder nun zu einer Kongruenz von der gleichen Form:

$$f_2(x) \equiv P''(x) \cdot f_3(x) \pmod{p} \tag{109}$$

führt, u. s. w. Da die Grade (mod. p) der Funktionen $f_1(x)$, $f_2(x)$, $f_3(x), \ldots$ stets abnehmen, kann dieser Prozefs nur ein endlicher sein, sodafs sich eine letzte Kongruenz

$$f_{k-1}(x) \equiv P^{(k-1)}(x) \cdot f_k(x) \pmod{p} \tag{110}$$

herausstellen mufs, in welcher $f_k(x)$ eine Primfunktion $P^{(k)}(x)$ (mod. p) ist. Durch die Verbindung der vorstehenden Kongruenzen (107) bis (110) ergiebt sich aber sogleich

$$f(x) \equiv P^0(x) \cdot P'(x) \cdot P''(x) \ldots P^{(k)}(x) \pmod{p}$$

d. h. die Zerlegung von $f(x)$ in Primfunktionen. Setzt man hier a_i als den Koeffizienten der höchsten Potenz von $P^{(i)}(x)$ voraus, so läfst sich $P^{(i)}(x) \equiv a_i P_i(x)$ (mod. p) setzen, wo jetzt $P_i(x)$ eine primäre Primfunktion ist, und die vorige Zerlegung von $f(x)$ nimmt die bestimmtere Form an:

$$f(x) \equiv \alpha \cdot P_0(x) P_1(x) P_2(x) \ldots P_k(x) \pmod{p}, \tag{111}$$

in welcher $\alpha \equiv a_0 a_1 a_2 \ldots a_k$ (mod. p) eine ganze zu p prime Zahl (eine Primfunktion nullten Grades) und allgemein $P_i(x)$ eine primäre Primfunktion bedeutet.

Die so als möglich nachgewiesene Zerlegung (111) der Funktion $f(x)$ in Primfunktionen ist zugleich eine eindeutig bestimmte; es kann mit anderen Worten nicht auch

$$f(x) \equiv \beta \cdot Q_0(x) Q_1(x) \ldots Q_h(x) \pmod{p} \tag{112}$$

sein, ohne dafs $h = k$, $\beta \equiv \alpha$ und die primären Primfunktionen $Q_0(x)$, $Q_1(x) \ldots Q_h(x)$, von einer etwa verschiedenen Anordnung abgesehen, den Primfunktionen $P_0(x)$, $P_1(x) \ldots P_k(x)$ (mod. p) gleich sind. Bestände nämlich eine solche zweite Zerlegung von $f(x)$, so schlösse man zunächst die Kongruenz

$$\beta Q_0(x) Q_1(x) \ldots Q_h(x) \equiv \alpha P_0(x) P_1(x) \ldots P_k(x) \pmod{p}. \tag{113}$$

Ihr zufolge wäre das Produkt zur Linken teilbar durch die Primfunktion $P_0(x)$; dies müfste also auch einer der Faktoren, etwa $Q_0(x)$, sein, eine Funktion, welche (mod. p) keine wesentlich von ihr verschiedene Funktion zum Teiler hat; da zudem sowohl $P_0(x)$ als $Q_0(x)$ eine primäre Funktion ist, mufs notwendig $Q_0(x) \equiv P_0(x)$ (mod. p) sein, die Kongruenz (113) nähme also die Gestalt

$$P_0(x) \cdot [\beta Q_1(x) \ldots Q_h(x) - \alpha P_1(x) \ldots P_k(x)] \equiv 0 \pmod{p}$$

und, da der erste Faktor nicht durch p teilbar ist, die einfachere Gestalt

$$\beta Q_1(x) \ldots Q_h(x) \equiv \alpha P_1(x) \ldots P_k(x) \pmod{p}$$

an, aus welcher wieder etwa $Q_1(x) \equiv P_1(x)$ zu schliefsen wäre, u. s. w. So würde jedem Faktor $P_i(x)$ ein kongruenter Faktor $Q_i(x)$ entsprechen also $h \overline{\gtrless} k$ sein müssen; aus gleicher Erwägung fände man aber auch umgekehrt $k \overline{\gtrless} h$ mithin $h = k$ und damit die völlige Übereinstimmung der Primfunktionen in beiden Zerlegungen; daher fände sich dann endlich aus (113) auch noch $\beta \equiv \alpha \pmod{p}$, wie behauptet.

Fafst man schliefslich in der Zerlegung (111) die etwa gleichen primären Primfunktionen immer zu einer Potenz zusammen, so findet sich der folgende fundamentale Satz: Jede ganze, ganzzahlige Funktion $f(x)$ von bestimmtem Grade kann stets und nur auf eine einzige Weise nach der Formel

$$(114) \qquad f(x) \equiv \alpha \cdot P_0(x)^h \cdot P_1(x)^{h_1} \ldots P_r(x)^{h_r} \pmod{p}$$

als Produkt aus einer ganzen Zahl in Potenzen primärer Primfunktionen dargestellt werden.

Schreibt man hierfür kurz

$$f(x) \equiv P_0(x)^h \cdot Q_0(x) \pmod{p},$$

eine Formel, welche — unter $F(x)$ eine gewisse ganze ganzzahlige Funktion verstanden — mit der folgenden:

$$f(x) = P_0(x)^h \cdot Q_0(x) + p \cdot F(x)$$

identisch ist, so erhält man durch ihre Differenzierung

$$f'(x) = P_0(x)^{h-1}[hP_0'(x)\,Q_0(x) + P_0(x)\,Q_0'(x)] + p \cdot F'(x)$$

oder kürzer

$$f'(x) \equiv P_0(x)^{h-1} \cdot Q_1(x) \pmod{p},$$

wo für $h = 1$ $\quad Q_1(x) = hP_0'(x)\,Q_0(x) + P_0(x)\,Q_0'(x)$

nicht (mod. p) durch $P_0(x)$ teilbar sein kann, da weder $Q_0(x)$ noch $P_0'(x)$ es ist, ersteres nach der Bedeutung von $Q_0(x)$, letzteres, weil $P_0'(x)$ geringeren Grades (mod. p) ist als $P_0(x)$; jenachdem also $h > 1$ oder $h = 1$ ist, d. h. jenachdem $f(x)$ den Primteiler $P_0(x)$ (mod. p) mehrfach enthält oder nicht, wird die abgeleitete Funktion $f'(x)$ diesen Primteiler auch haben oder ihn nicht haben. Hieraus folgt der Satz: Hat eine Funktion $f(x)$ (mod. p) einen Teiler mehrfach, so hat sie mit ihrer Abgeleiteten $f'(x)$ (mod. p) einen gemeinsamen Teiler, und umgekehrt. In der That, wenn $f(x)$ einen Teiler mehrfach hat, so hat es auch jeden Primteiler $P_0(x)$ desselben mehrfach und diesen also nach dem eben Bewiesenen gemeinsam mit $f'(x)$; umgekehrt, wenn $f(x)$, $f'(x)$ einen (mod. p) gemeinsamen Teiler haben, so haben sie auch jeden Primteiler $P_0(x)$ desselben gemeinsam, letzterer aber mufs in $f(x)$ mehrfach aufgehen, da sonst $f'(x)$ nach dem Voraufgehenden ihn nicht haben würde.

21. Zunächt werde nun der Nachweis geführt, dafs es (mod. p) Primfunktionen von jedem beliebig gegebenen Grade m giebt, und

die Anzahl inkongruenter primärer Primfunktionen dieses Grades ermittelt. Wir folgen dabei an dieser Stelle der von Gaufs (*art.* 342 bis 347) angegebenen analytischen Methode.

Bezeichne (m) die Anzahl aller inkongruenten primären Primfunktionen vom Grade m, die möglicherweise auch Null sein kann, (m^a) aber die Anzahl aller inkongruenten primären Funktionen, welche aus a kongruenten oder inkongruenten primären Primfunktionen m^{ten} Grades zusammengesetzt sind; dann ist offenbar

$$(115)\qquad (m^a) = \frac{(m)\cdot\overline{(m)+1}\cdot\overline{(m)+2}\cdots\overline{(m)+a-1}}{1\cdot 2\cdot 3\cdots a}.$$

Die Anzahl aller inkongruenten primären Funktionen, welche aus irgend welchen a primären Primfunktionen vom Grade m, aus irgend welchen a' primären Primfunktionen vom Grade m', u. s. w. zusammengesetzt sind, beträgt ersichtlich $(m^a)\cdot(m'^{a'})\ldots$; bezeichnet man also dieselbe Anzahl mit $(m^a\cdot m'^{a'}\ldots)$, so besteht die Beziehung

$$(116)\qquad (m^a\cdot m'^{a'}\cdots) = (m^a)\cdot(m'^{a'})\cdots$$

Sei nun $f(x)$ eine beliebige primäre Funktion vom Grade m, so darf eine solche (mod. p) stets als zusammengesetzt gedacht werden aus α von den (1) existierenden inkongruenten primären Primfunktionen vom Grade 1, aus β der vorhandenen (2) inkongruenten primären Primfunktionen vom Grade 2, aus γ der (3) inkongruenten primären Primfunktionen vom Grade 3, u. s. w., wo die Zahlen $\alpha, \beta, \gamma, \ldots$, welche Null oder positiv sein dürfen, die Bedingung

$$(117)\qquad 1\cdot\alpha + 2\cdot\beta + 3\cdot\gamma + \cdots = m$$

erfüllen. Jeder solchen Lösung $\alpha, \beta, \gamma, \ldots$ vorstehender Gleichung entsprechen $(1^\alpha\, 2^\beta\, 3^\gamma\ldots)$ inkongruente primäre Funktionen vom Grade m; die Anzahl aller inkongruenten primären Funktionen dieses Grades drückt sich folglich durch die auf alle jene Lösungen bezogene Summe $S(1^\alpha\, 2^\beta\, 3^\gamma\ldots)$ aus, und da sie von uns bereits gleich p^m gefunden worden ist, so ergiebt sich mit Rücksicht auf (116) die folgende Formel:

$$(118)\qquad p^m = S(1^\alpha)\cdot(2^\beta)\cdot(3^\gamma)\cdots;$$

in welcher die Summation den gleichen Umfang hat wie zuvor.

Nun besteht die für jedes $x < 1$ konvergente Reihenentwicklung

$$\left(\frac{1}{1-x^d}\right)^{(d)} = \sum_{\delta=0}^{\infty} \frac{(d)\cdot\overline{(d)+1}\cdots\overline{(d)+\delta-1}}{1\cdot 2\cdots\delta}\cdot x^{d\delta}$$

oder nach (115) und, wenn man $(d^0) = 1$ festsetzt,

$$\left(\frac{1}{1-x^d}\right)^{(d)} = \sum_{\delta=0}^{\infty} (d^\delta)\cdot x^{d\delta},$$

mithin ist

aufstellen, in welcher $q(x)$, $r(x)$ ganze, ganzzahlige Funktionen, die letztere von geringerem Grade als $\varphi(x)$, bezeichnen; solcher (mod. p) inkongruenter Funktionen $r(x)$ giebt es aber nur p^μ und einer von ihnen ist der vorigen Kongruenz zufolge, welche mit einer Gleichung, wie sie folgt:

$$f(x) = \varphi(x)\, q(x) + r(x) + p\chi(x)$$

identisch ist, jede Funktion (modd. p, $\varphi(x)$) kongruent. Zwei Funktionen nun, welche ein- und derselben dieser p^μ Funktionen $r(x)$ nach jenem Doppelmodulus kongruent sind, werden, wie bemerkt, es auch unter einander sein; dagegen werden sie inkongruent sein (modd. p, $\varphi(x)$), wenn sie zwei verschiedenen jener p^μ Funktionen, etwa $r(x)$, $r_1(x)$ kongruent sind, denn sonst müfste auch

$$r(x) \equiv r_1(x) \text{ (modd. } p, \varphi(x))$$

d. h. $r(x) - r_1(x)$ (mod. p) durch $\varphi(x)$ teilbar sein, was, da der Grad jener Differenz geringer ist als der von $\varphi(x)$, nur geschehen könnte, wenn $r(x) \equiv r_1(x)$ (mod. p) wäre, gegen die Voraussetzung. Hiernach giebt es soviel inkongruente Funktionen $f(x)$ (modd. p, $\varphi(x)$), als es verschiedene Funktionen $r(x)$ giebt, d. h. p^μ, w. z. b. w.

Nun bezeichne $P(x)$ eine (primäre) Primfunktion (mod. p) vom Grade m. Dann giebt es p^m (modd. p, $P(x)$) inkongruente Funktionen $f(x)$. Eine einzige von diesen ist (mod. p) teilbar durch $P(x)$, denn aus der mit (129) analogen Kongruenz

$$f(x) \equiv P(x)\; Q(x) + R(x) \text{ (mod. } p)$$

ergiebt sich $f(x)$ (mod. p) teilbar durch $P(x)$ dann und nur dann, wenn die Restfunktion $R(x) \equiv 0$ (mod. p). Bezeichnet man daher mit

$$(130) \qquad f_1(x),\ f_2(x), \cdots f_{p^m-1}(x)$$

die $p^m - 1$ übrigen der (modd. p, $P(x)$) inkongruenten Funktionen, von denen wir sagen wollen, dafs sie ein reduziertes Restsystem (modd. p, $P(x)$) bilden, so sind diese, weil durch $P(x)$ nicht teilbar (mod. p), relative Primfunktionen zu $P(x)$. Dasselbe gilt dann nach Ende von Nr. 19, falls $f(x)$ irgend eine zu $P(x)$ prime Funktion bedeutet, auch von den $p^m - 1$ Produkten

$$(131) \qquad f(x) f_1(x),\ f(x) f_2(x), \cdots f(x) f_{p^m-1}(x),$$

welche zudem wieder ein reduziertes Restsystem (modd. p, $P(x)$) bilden, da je zwei von ihnen nach diesem Doppelmodulus inkongruent sind; denn, wäre z. B.

$$f(x) f_1(x) \equiv f(x) f_2(x) \text{ (modd. } p, P(x)),$$

so ergäbe sich $f(x) \cdot (f_1(x) - f_2(x))$ und somit auch $f_1(x) - f_2(x)$ (mod. p) teilbar durch $P(x)$ d. h.

$$f_1(x) \equiv f_2(x) \text{ (modd. } p, P(x))$$

gegen die Voraussetzung. Hiernach müssen die Funktionen (131), von der Ordnung abgesehen, den Funktionen (130) und somit auch das Produkt der ersteren dem der letzteren (modd. p, $P(x)$) kongruent sein, in Zeichen:

$$f(x)^{p^m-1} \cdot f_1(x) f_2(x) \cdots f_{p^m-1}(x) \equiv f_1(x) f_2(x) \cdots f_{p^m-1}(x)$$

oder

$$(f(x)^{p^m-1} - 1) \cdot f_1(x) f_2(x) \cdots f_{p^m-1}(x) \equiv 0 \pmod{p, P(x)}$$

d. h. durch $P(x)$ (mod. p) teilbar sein; da der zweite Faktor relativ prim zu $P(x)$ ist, mufs der erste Faktor teilbar oder

$$(132) \qquad f(x)^{p^m-1} \equiv 1 \quad (\text{modd. } p, P(x))$$

sein.

Jede durch die Primfunktion $P(x)$ vom Grade m (mod. p) nicht teilbare Funktion $f(x)$ leistet also der Kongruenz (132) Genüge. Dieser Kongruenz, welche in der Theorie der höheren Kongruenzen genau die Stelle des Fermatschen Satzes vertritt und daher auch als solcher benannt werden mag, kann, analog wie dem letzteren, eine Form gegeben werden, in der sie für jede Funktion, auch für solche, die durch $P(x)$ teilbar sind, Geltung hat. In der That folgt aus (132) die andere Kongruenz:

$$(133) \qquad f(x)^{p^m} \equiv f(x) \quad (\text{modd. } p, P(x)),$$

und diese besteht offenbar auch noch, wenn $f(x)$ (mod. p) durch $P(x)$ aufgeht.

Man darf schliefslich also den Satz aussprechen: Ist $P(x)$ eine Primfunktion (mod. p) vom Grade m, so ist jede der p^m (modd. p, $P(x)$) inkongruenten Funktionen $f(x)$ eine Wurzel der Kongruenz

$$(134) \qquad X^{p^m} \equiv X \quad (\text{modd. } p, P(x)),$$

welche demnach in Bezug auf diesen Doppelmodulus genau soviel Wurzeln hat, als ihr Grad beträgt.

Hier fügt sich passend der allgemeine Satz an, dafs eine Kongruenz

$$(135) \qquad F(X) \equiv 0 \quad (\text{modd. } p, P(x)),$$

in welcher

$$(136) \qquad F(X) = AX^M + A_1 X^{M-1} + \cdots + A_{M-1} X + A_M$$

eine ganze Funktion von X und die Koeffizienten A_i ganze, ganzzahlige Funktionen von x oder auch ganze Zahlen sind, nicht mehr Wurzeln haben kann, als ihr Grad beträgt; unter dieser Benennung aber wird der Exponent des höchsten Gliedes verstanden, dessen Koeffizient eine (mod. p) durch $P(x)$ nicht teilbare

aufstellen, in welcher $q(x)$, $r(x)$ ganze, ganzzahlige Funktionen, die letztere von geringerem Grade als $\varphi(x)$, bezeichnen; solcher (mod. p) inkongruenter Funktionen $r(x)$ giebt es aber nur p^μ und einer von ihnen ist der vorigen Kongruenz zufolge, welche mit einer Gleichung, wie sie folgt:

$$f(x) = \varphi(x)\, q(x) + r(x) + p\,\chi(x)$$

identisch ist, jede Funktion (modd. p, $\varphi(x)$) kongruent. Zwei Funktionen nun, welche ein- und derselben dieser p^μ Funktionen $r(x)$ nach jenem Doppelmodulus kongruent sind, werden, wie bemerkt, es auch unter einander sein; dagegen werden sie inkongruent sein (modd. p, $\varphi(x)$), wenn sie zwei verschiedenen jener p^μ Funktionen, etwa $r(x)$, $r_1(x)$ kongruent sind, denn sonst müfste auch

$$r(x) \equiv r_1(x) \pmod{p,\ \varphi(x)}$$

d. h. $r(x) - r_1(x)$ (mod. p) durch $\varphi(x)$ teilbar sein, was, da der Grad jener Differenz geringer ist als der von $\varphi(x)$, nur geschehen könnte, wenn $r(x) \equiv r_1(x)$ (mod. p) wäre, gegen die Voraussetzung. Hiernach giebt es soviel inkongruente Funktionen $f(x)$ (modd. p, $\varphi(x)$), als es verschiedene Funktionen $r(x)$ giebt, d. h. p^μ, w. z. b. w.

Nun bezeichne $P(x)$ eine (primäre) Primfunktion (mod. p) vom Grade m. Dann giebt es p^m (modd. p, $P(x)$) inkongruente Funktionen $f(x)$. Eine einzige von diesen ist (mod. p) teilbar durch $P(x)$, denn aus der mit (129) analogen Kongruenz

$$f(x) \equiv P(x)\, Q(x) + R(x) \pmod{p}$$

ergiebt sich $f(x)$ (mod. p) teilbar durch $P(x)$ dann und nur dann, wenn die Restfunktion $R(x) \equiv 0$ (mod. p). Bezeichnet man daher mit

$$(130) \qquad f_1(x),\ f_2(x),\ \cdots\ f_{p^m-1}(x)$$

die $p^m - 1$ übrigen der (modd. p, $P(x)$) inkongruenten Funktionen, von denen wir sagen wollen, dafs sie ein reduziertes Restsystem (modd. p, $P(x)$) bilden, so sind diese, weil durch $P(x)$ nicht teilbar (mod. p), relative Primfunktionen zu $P(x)$. Dasselbe gilt dann nach Ende von Nr. 19, falls $f(x)$ irgend eine zu $P(x)$ prime Funktion bedeutet, auch von den $p^m - 1$ Produkten

$$(131) \qquad f(x)\, f_1(x),\ f(x)\, f_2(x),\ \cdots\ f(x)\, f_{p^m-1}(x),$$

welche zudem wieder ein reduziertes Restsystem (modd. p, $P(x)$) bilden, da je zwei von ihnen nach diesem Doppelmodulus inkongruent sind; denn, wäre z. B.

$$f(x)\, f_1(x) \equiv f(x)\, f_2(x) \pmod{p,\ P(x)},$$

so ergäbe sich $f(x) \cdot (f_1(x) - f_2(x))$ und somit auch $f_1(x) - f_2(x)$ (mod. p) teilbar durch $P(x)$ d. h.

$$f_1(x) \equiv f_2(x) \pmod{p,\ P(x)}$$

gegen die Voraussetzung. Hiernach müssen die Funktionen (131), von der Ordnung abgesehen, den Funktionen (130) und somit auch das Produkt der ersteren dem der letzteren (modd. p, $P(x)$) kongruent sein, in Zeichen:

$$f(x)^{p^m-1} \cdot f_1(x)\, f_2(x) \cdots f_{p^m-1}(x) \equiv f_1(x)\, f_2(x) \cdots f_{p^m-1}(x)$$

oder

$$(f(x)^{p^m-1} - 1) \cdot f_1(x)\, f_2(x) \cdots f_{p^m-1}(x) \equiv 0 \;(\text{modd.}\, p,\, P(x))$$

d. h. durch $P(x)$ (mod. p) teilbar sein; da der zweite Faktor relativ prim zu $P(x)$ ist, mufs der erste Faktor teilbar oder

$$(132) \qquad f(x)^{p^m-1} \equiv 1 \;(\text{modd.}\, p,\, P(x))$$

sein.

Jede durch die Primfunktion $P(x)$ vom Grade m (mod. p) nicht teilbare Funktion $f(x)$ leistet also der Kongruenz (132) Genüge. Dieser Kongruenz, welche in der Theorie der höheren Kongruenzen genau die Stelle des Fermatschen Satzes vertritt und daher auch als solcher benannt werden mag, kann, analog wie dem letzteren, eine Form gegeben werden, in der sie für jede Funktion, auch für solche, die durch $P(x)$ teilbar sind, Geltung hat. In der That folgt aus (132) die andere Kongruenz:

$$(133) \qquad f(x)^{p^m} \equiv f(x) \;(\text{modd.}\, p,\, P(x)),$$

und diese besteht offenbar auch noch, wenn $f(x)$ (mod. p) durch $P(x)$ aufgeht.

Man darf schliefslich also den Satz aussprechen: Ist $P(x)$ eine Primfunktion (mod. p) vom Grade m, so ist jede der p^m (modd. p, $P(x)$) inkongruenten Funktionen $f(x)$ eine Wurzel der Kongruenz

$$(134) \qquad X^{p^m} \equiv X \;(\text{modd.}\, p,\, P(x)),$$

welche demnach in Bezug auf diesen Doppelmodulus genau soviel Wurzeln hat, als ihr Grad beträgt.

Hier fügt sich passend der allgemeine Satz an, dafs eine Kongruenz

$$(135) \qquad F(X) \equiv 0 \;(\text{modd.}\, p,\, P(x)),$$

in welcher

$$(136) \qquad F(X) = AX^M + A_1 X^{M-1} + \cdots + A_{M-1} X + A_M$$

eine ganze Funktion von X und die Koeffizienten A_i ganze, ganzzahlige Funktionen von x oder auch ganze Zahlen sind, nicht mehr Wurzeln haben kann, als ihr Grad beträgt; unter dieser Benennung aber wird der Exponent des höchsten Gliedes verstanden, dessen Koeffizient eine (mod. p) durch $P(x)$ nicht teilbare

Funktion ist. Hätte nämlich die Kongruenz (135) M^{ten} Grades mehr als M, mithin mindestens $M+1$ Wurzeln:

$$X_1, X_2, \ldots X_M, X_{M+1},$$

so bilde man den Ausdruck

$$G(X) = A(X-X_1)(X-X_2)\ldots(X-X_M)$$

und vermittelst desselben die Differenz

$$F(X) - G(X),$$

welche eine wie $F(X)$ geartete ganze Funktion von X höchstens noch vom Grade $M-1$ sein wird. Die Kongruenz

$$(137) \qquad F(X) - G(X) \equiv 0 \pmod{p, P(x)}$$

hat dann ersichtlich die M Wurzeln $X_1, X_2, \ldots X_M$; nehmen wir daher den behaupteten Satz als bereits feststehend an für alle Kongruenzen von kleinerem Grade als M, so mufs die Kongruenz (137) identisch, d. h. für jede ganze Funktion X von x bestehen und somit mufs auch

$$F(X_{M+1}) - G(X_{M+1}) \equiv 0$$

d. h.

$$A\cdot(X_{M+1}-X_1)(X_{M+1}-X_2)\cdots(X_{M+1}-X_M) \equiv 0$$

sein, also müfste, da A nicht (mod. p) durch $P(x)$ teilbar ist, es einer der übrigen Faktoren und folglich X_{M+1} mit einer der Funktionen $X_1, X_2, \ldots X_M$ (modd. p, $P(x)$) kongruent sein, was der Voraussetzung zuwider ist.

Dem Fermatschen Satze (132) entsprechend hat nun die Kongruenz

$$X^{p^m-1} - 1 \equiv 0 \pmod{p, P(x)}$$

die sämtlichen Glieder eines reduzierten Restsystems d. i. die p^m-1 Funktionen (130) zu Wurzeln; man erschliefst daher durch die voraufgehende Betrachtung die identische Kongruenz

$$X^{p^m-1} - 1 - (X-f_1(x))(X-f_2(x))\ldots(X-f_{p^m-1}(x)) \equiv 0$$

und, wenn hier $X=0$ gewählt wird, die folgende Beziehung:

$$(138) \qquad f_1(x)f_2(x)\ldots f_{p^m-1}(x) \equiv -1 \pmod{p, P(x)},$$

welche das Analogon des Wilsonschen Satzes ist, insofern sie aussagt, dafs das Produkt aller Glieder eines reduzierten Restsystems (modd. p, $P(x)$) nach diesem Doppelmodulus der negativen Einheit kongruent ist.

23. Aber wir verfolgen nun die Konsequenzen aus dem Fermatschen Satze in anderer Richtung. Wählt man in der für jede ganze ganzzahlige Funktion giltigen Kongruenz (133) $f(x) = x$, so kommt

$$x^{p^m} \equiv x \pmod{p, P(x)},$$

ein Resultat, welches man folgendermafsen aussprechen kann: Jede (mod. p) irreduktible Funktion m^{ten} Grades ist (mod. p) ein Teiler der Funktion $x^{p^m}-x$.

Es ist hiernach nicht schwierig, diese letztere Funktion überhaupt in ihre irreduktiblen Faktoren (mod. p) zu zerlegen. Wir haben dazu nur noch einen einfachen Hilfssatz vorauszuschicken. Ist $f(x)$ eine beliebige ganze, ganzzahlige Funktion von x:

$$f(x) = ax^h + a_1 x^{h-1} + \cdots + a_{h-1}x + a_h,$$

so giebt nach den Eigenschaften der Polynomialkoeffizienten (Kap. 2, Nr. 12) ihre Erhebung zur p^{ten} Potenz unmittelbar die Kongruenz

$$f(x)^p \equiv a^p x^{hp} + a_1^p x^{(h-1)p} + \cdots + a_{h-1}^p x^p + a_h^p \pmod{p}$$

und wegen des Fermatschen Satzes noch einfacher:

$$f(x)^p \equiv ax^{hp} + a_1 x^{(h-1)p} + \cdots + a_{h-1} x^p + a_h \pmod{p}$$

d. h.

$$f(x)^p \equiv f(x^p) \pmod{p},$$

eine Beziehung, welche durch Wiederholung der gleichen Operation sich verallgemeinern läfst zu der Formel

$$f(x)^{p^m} \equiv f(x^{p^m}) \pmod{p}, \tag{139}$$

welche den gedachten Hilfssatz zum Ausdrucke bringt.

1) Durch ihn beweist man sogleich, dafs die Funktion $x^{p^m} - x$ (mod. p) keine Primfunktion von höherem als dem m^{ten} Grade als Teiler besitzt. Wäre nämlich eine Primfunktion $\Pi(x)$ vom Grade $k > m$ ein Teiler jenes Ausdrucks, also

$$x^{p^m} - x \equiv 0 \quad (\text{modd. } p,\ \Pi(x)),$$

so ergäbe die auch für diesen Doppelmodulus giltige Kongruenz (139) für jede der (modd. p, $\Pi(x)$) vorhandenen p^k Restfunktionen $f(x)$ die Folgerung

$$f(x)^{p^m} \equiv f(x) \quad (\text{modd. } p,\ \Pi(x)),$$

die Kongruenz

$$X^{p^m} \equiv X \quad (\text{modd. } p,\ \Pi(x))$$

hätte also mehr Wurzeln als ihr Grad beträgt, gegen den zuvor bewiesenen allgemeinen Kongruenzsatz.

2) Ist dagegen $\Pi(x)$ eine Primfunktion, deren Grad $d<m$ ist, so wird sie gewifs ein Teiler (mod. p) von $x^{p^m} - x$ sein, wenn d aufgeht in m. Denn, da nach dem Fermatschen Satze

$$x^{p^d} \equiv x \quad (\text{modd. } p,\ \Pi(x))$$

ist, so folgt allgemeiner für jedes Vielfache hd von d

$$x^{p^{hd}} \equiv x$$

und somit auch
$$x^{p^m} \equiv x \text{ (modd. } p,\ \Pi(x)).$$

3) Andererseits kann $x^{p^m} - x$ auch nur Primfunktionen solcher Grade $d < m$ zu Teilern haben, bei welchen d in m aufgeht. Denn, wäre im Gegenteil $m = dq + r$, wo $0 < r < d$, so folgte aus dem gleichzeitigen Bestehen der Kongruenzen
$$x^{p^m} \equiv x, \quad x^{p^d} \equiv x \text{ (modd. } p,\ \Pi(x))$$
leicht auch die folgende
$$x^{p^r} \equiv x \text{ (modd. } p,\ \Pi(x)),$$
die Funktion $x^{p^r} - x$ hätte also dem unter 1) Bewiesenen entgegen die Primfunktion $\Pi(x)$ (mod. p) von höherem als dem r^{ten} Grade zum Teiler.

Aus diesen Punkten ist zu erschliefsen, dafs die Funktion $x^{p^m} - x$ alle diejenigen Primfunktionen und nur diejenigen (mod. p) zu Teilern hat, deren Grade gleich m oder ein Teiler von m sind. Sie enthält aber endlich jeden dieser Primteiler auch nur einfach. Denn $x^{p^m} - x$ und die Ableitung dieser Funktion, $p^m x^{p^m - 1} - 1$, haben, da
$$p^m \cdot (x^{p^m} - x) - x \cdot (p^m x^{p^m - 1} - 1) = x(1 - p^m),$$
und x kein gemeinsamer Teiler derselben ist, überhaupt keinen solchen.

Beschränkt man sich zudem auf die Betrachtung primärer Primteiler, so folgert man aus alle diesem den nachstehenden Satz:

Die Funktion $x^{p^m} - x$ ist (mod. p) kongruent dem Produkte aller inkongruenten primären Primfunktionen, deren Grade gleich m oder ein Teiler von m sind.

Sei d jeder Teiler von m, m inklusive, und $P_d'(x)$, $P_d''(x)$, $P_d'''(x), \ldots$ die (d) inkongruenten primären Primfunktionen d^{ten} Grades (mod. p), endlich
$$\Phi_d(x) = P_d'(x) \cdot P_d''(x) \cdot P_d'''(x), \ldots, \tag{140}$$
so spricht sich der erhaltene wichtige Satz in Zeichen folgendermafsen aus: Es ist
$$x^{p^m} - x \equiv \prod_d \Phi_d(x) \text{ (mod. } p), \tag{141}$$
wenn hier die Multiplikation auf alle Teiler d von m, m inklusive, erstreckt gedacht wird.

Da der Grad (mod. p) eines Produkts gleich der Summe der Grade seiner Faktoren ist, ergiebt sich hieraus sogleich die Beziehung:
$$p^m \equiv \sum_d d(d), \tag{142}$$
in welcher die Summation den gleichen Umfang hat, wie vorher die Multiplikation; wir haben also die Formel (120), welche bisher nur

mit Hilfe analytischer Betrachtungen gewonnen worden war, jetzt auf rein arithmetischem Wege bestätigt.

Mittels desselben allgemeinen Satzes, der aus dieser Formel den Ausdruck (122) für die Anzahl (m) der inkongruenten primären Primfunktionen m^{ten} Grades herzuleiten verstattete, vermag man aus (141) auch deren Produkt $\Phi_m(x)$ zu entwickeln. Setzt man nämlich

$$\prod_d \Phi_d(x) = \Psi_m(x) \tag{143}$$

und folglich

$$\sum_d \log\, \Phi_d(x) = \log\, \Psi_m(x),$$

so ist dies eine Beziehung zwischen der ganzen Zahl m und ihren sämtlichen Teilern ganz von derselben Art, wie sie in der Formel (52) des 3. Kapitels zum Ausdrucke kommt, und demgemäfs ist, wenn man für m wieder die Zerlegung (121) voraussetzt, aus ihr die folgende:

$$\log\, \Phi_m(x) = \log\, \Psi_m(x) - \sum \log\, \Psi_{\frac{m}{a}}(x) + \sum \log\, \Psi_{\frac{m}{ab}}(x) - \cdots$$

oder auch diese:

$$\Phi_m(x) = \frac{\Psi_m(x) \cdot \Pi\, \Psi_{\frac{m}{ab}}(x) \cdots}{\Pi\, \Psi_{\frac{m}{a}}(x) \cdot \Pi\, \Psi_{\frac{m}{abc}}(x) \cdots}$$

zu erschliefsen. Giebt man der letzteren die Form

$$\Phi_m(x) \cdot \prod \Psi_{\frac{m}{a}}(x) \cdots = \Psi_m(x) \cdot \prod \Psi_{\frac{m}{ab}}(x) \cdots,$$

so liest sich daraus mit Rücksicht auf (141) und (143) die Kongruenz

$$\Phi_m(x) \cdot \prod \left(x^{p^{\frac{m}{a}}} - x\right) \cdots \equiv \left(x^{p^m} - x\right) \cdot \prod \left(x^{p^{\frac{m}{ab}}} - x\right) \cdots \pmod{p}$$

und nun, wie sogleich zu ersehen, die Formel

$$\Phi_m(x) \equiv \frac{\left(x^{p^m} - x\right) \cdot \Pi \left(x^{p^{\frac{m}{ab}}} - x\right) \cdots}{\Pi \left(x^{p^{\frac{m}{a}}} - x\right) \Pi \left(x^{p^{\frac{m}{abc}}} - x\right) \cdots} \pmod{p} \tag{144}$$

ab, wenn sich nachweisen läfst, dafs der Ausdruck zur Rechten, den wir kurz durch $F(x)$ bezeichnen wollen, eine ganze, ganzzahlige Funktion von x ist.

Um diesen Nachweis zu führen, bemerke man zuvörderst, dafs, wenn unter k die Anzahl der verschiedenen Primfaktoren $a, b, c, \ldots$ von m verstanden wird, der Faktor x sich im Zähler von $F(x)$

$$1 + \frac{k(k-1)}{1 \cdot 2} + \frac{k(k-1)(k-2)(k-3)}{1 \cdot 2 \cdot 3 \cdot 4} + \cdots,$$

im Nenner dagegen

$$\frac{k}{1} + \frac{k(k-1)(k-2)}{1 \cdot 2 \cdot 3} + \cdots$$

Mal, d. h., da der Unterschied beider Ausdrücke gleich $(1-1)^k = 0$ ist, sich im Zähler und Nenner gleich oft finden und daher aus dem Bruche fortheben wird. Ist ferner $x - \alpha$ irgend ein von x verschiedener Linearfaktor des Nenners also einer der darin vorhandenen Differenzen

$$x^{p^{\frac{m}{a}}} - x, \ldots, \quad x^{p^{\frac{m}{abc}}} - x, \ldots,$$

so ist er, da die Exponenten $\frac{m}{a}, \ldots, \frac{m}{abc}, \ldots$ der Potenzen von p sämtlich Teiler von m sind, auch ein Linearfaktor von $x^{p^m} - x$. Sei nun für irgend einen Linearfaktor von $x^{p^m} - x$ unter allen Ausdrücken der gleichen Form $x^{p^d} - x$ derjenige geringsten Grades, welcher denselben ebenfalls besitzt; dann wird jener Linearfaktor offenbar auch ein Faktor von jeder Differenz $x^{p^\delta} - x$ und nur von solchen sein, bei welchen δ ein Vielfaches von d ist, und folglich wird d, da auch $x^{p^m} - x$ jenen Linearfaktor haben soll, ein Teiler von m sein. Ein solcher enthält, wenn er kleiner als m ist, eine gewisse Anzahl — sie heifse h — von den Primfaktoren von m weniger oft als m. Dann sind genau h der Zahlen $\frac{m}{a}, \frac{m}{b}, \frac{m}{c}, \cdots$ durch d teilbar, von den Zahlen $\frac{m}{ab}, \frac{m}{ac}, \cdots$ genau $\frac{h(h-1)}{1 \cdot 2}$, von den Zahlen $\frac{m}{abc}, \cdots$ genau $\frac{h(h-1)(h-2)}{1 \cdot 2 \cdot 3}$, u. s. w., und nach derselben Überlegung wie zuvor findet sich, dafs der gedachte Linearfaktor im Zähler wie im Nenner von $F(x)$ gleich oft auftritt, sich also weghebt. Da dies für jeden Linearfaktor $x - \alpha$ des Nenners der Fall ist, hebt sich ein jeder solcher aus dem Bruche fort, d. h. der Ausdruck $F(x)$ ist in der That eine ganze Funktion, deren Koeffizienten zudem ganze Zahlen sein müssen, da die höchsten Koeffizienten der Divisoren der Einheit gleich sind.

24. Die so erhaltenen Resultate, betreffend die Zerlegung der Ausdrücke von der Form $x^{p^m} - x$ in Primfunktionen (mod. p) können nun benutzt werden, auf eine theoretisch sehr einfache Weise für jede beliebige ganze, ganzzahlige Funktion $f(x)$ ihre Primteiler (mod. p) zu ermitteln. Dabei darf man der Einfachheit halber voraussetzen, dafs $f(x)$ keine mehrfachen Primteiler habe, da andernfalls diese aus ihrem (mod. p) mit der Abgeleiteten $f'(x)$ gemeinsamen Teiler bestimmbar sein würden. Da nun $x^p - x$ das Produkt sämtlicher (inkongruenter) Primfunktionen ersten Grades (mod. p) ist, also aufser ihnen keine Primteiler weiter besitzt, so wird man ersichtlich das Produkt aller Primteiler ersten Grades, welche $f(x)$ hat, erhalten, wenn man durch den in Nr. 19 angegebenen Al-

gorithmus den gröfsten gemeinsamen Teiler $F_1(x)$ von $f(x)$ und $x^p - x$ (mod. p) bestimmt. Setzt man alsdann

$$f(x) \equiv F_1(x) \cdot f_1(x) \pmod{p},$$

so kann $f_1(x)$ keine Primteiler ersten Grades mehr enthalten, enthält dagegen jeden Primteiler von $f(x)$, der höheren Grades ist. Da ferner $x^{p^2} - x$ aufser Primteilern ersten Grades die sämtlichen Primfunktionen zweiten Grades (mod. p) zu Teilern hat, so findet man offenbar das Produkt aller Primteiler zweiten Grades (mod. p) von $f(x)$ d. h. von $f_1(x)$, wenn man den gröfsten gemeinsamen Teiler $F_2(x)$ von $f_1(x)$ und $x^{p^2} - x$ (mod. p) ermittelt. Wenn alsdann

$$f_1(x) \equiv F_2(x) \cdot f_2(x) \pmod{p}$$

also

$$f(x) \equiv F_1(x)\, F_2(x) f_2(x)$$

gesetzt wird, so enthält $f_2(x)$ noch jeden aber auch nur jeden Primfaktor von $f(x)$, dessen Grad (mod. p) höher als 2 ist. Um daher das Produkt der Primteiler dritten Grades von $f(x)$ zu finden, hat man wieder nur den gröfsten gemeinsamen Teiler $F_3(x)$ von $f_2(x)$ und $x^{p^3} - x$ (mod. p) zu bestimmen, u. s. w. fort. Da hierbei die Grade der Funktionen $f(x)$, $f_1(x)$, $f_2(x)$, ... (mod. p) eine abnehmende Reihe ganzer Zahlen bilden, mufs der Prozefs ein endlicher sein, man also zuletzt auf eine Kongruenz

$$f(x) \equiv F_1(x)\, F_2(x)\, F_3(x) \ldots F_n(x) \pmod{p}$$

geführt werden, in welcher allgemein $F_i(x)$ das Produkt aller Primteiler i^{ten} Grades von $f(x)$ bedeutet.

Um nun noch jedes Produkt $F_i(x)$ in seine Primfunktionen zerlegt darzustellen, nehme man den allgemeinen Ausdruck i^{ten} Grades

$$F(x) = x^i + A_1 x^{i-1} + \cdots + A_{i-1} x + A_i$$

mit zunächst unbestimmten Koeffizienten und teile die Funktion $F_i(x)$ algebraisch durch ihn, sodafs sich

$$F_i(x) = F(x) \cdot Q(x) + R(x)$$

ergiebt, wo $R(x)$ eine ganze Funktion $i-1^{\text{ten}}$ Grades ist mit Koeffizienten, welche lineare, ganzzahlige Funktionen der i unbestimmten Gröfsen $A_1, A_2, \ldots A_i$ sein müssen. Damit dann $F(x)$ ein ganzzahliger Teiler (mod. p) von $F_i(x)$ d. i. einer der Primteiler dieses Produkts werde, ist offenbar notwendig und hinreichend, dafs jene Gröfsen die i Kongruenzen erfüllen, welche man erhält, indem man die i Koeffizienten von $R(x)$ (mod. p) kongruent Null setzt. Diese i Kongruenzen müssen genau soviel ganzzahlige Lösungen gestatten, als die Anzahl der Primteiler von $F_i(x)$ beträgt, welche man also auf solche Weise sämtlich einzeln erhält (Serret, Nr. 351).

25. So einfach in theoretischer Hinsicht diese Methode auch ist, so wenig empfiehlt sie sich in praktischer Beziehung. Um insbesondere die Ausdrücke von der Form

$$x^n - 1$$

(mod. p) in Primfunktionen zu zerlegen, werden wir andere Betrachtungen verwenden, die auch an sich für die hier entwickelte Theorie der Kongruenzen (modd. p, $P(x)$) von Interesse sind.

Für jede ganze, ganzzahlige Funktion $f(x)$, welche (mod. p) durch die Primfunktion $P(x)$ nicht teilbar ist, giebt es eine gewisse niedrigste Potenz $f(x)^\delta$ so beschaffen, dafs

$$f(x)^\delta \equiv 1 \pmod{p, P(x)}$$

ist; und der Exponent δ derselben — wir wollen sagen: der Exponent, zu welchem $f(x)$ (modd. p, $P(x)$) gehört — ist ein Teiler von $p^m - 1$, wenn wieder m den Grad der Primfunktion $P(x)$ bezeichnet. Diesen Satz, der auch direkt durch sogenannte Exhaustion erwiesen werden kann (s. Dedekind, Nr. 13), folgert man am einfachsten aus dem Fermatschen Satze. Denn dem letztern zufolge ist jedenfalls $f(x)^{p^m-1}$ eine der Einheit kongruente Potenz; ist aber unter allen Potenzen dieser Art $f(x)^\delta$ die niedrigste, so schliefst man sehr leicht, dafs auch jede solche Potenz von $f(x)$, aber auch nur solche, deren Exponent ein Vielfaches von δ ist, der Einheit kongruent sein wird; da $f(x)^{p^m-1}$ eine solche Potenz ist, mufs $p^m - 1$ ein Vielfaches von δ sein, w. z. b. w.

Ist andererseits δ ein Teiler von $p^m - 1$ und giebt es eine Funktion $f(x)$, welche zu diesem Teiler als Exponenten gehört, so müssen die δ Potenzen

$$f(x),\ f(x)^2,\ f(x)^3, \ldots f(x)^\delta \tag{145}$$

offenbar (modd. p, $P(x)$) inkongruent sein und da sie mit $f(x)$ zugleich sämtlich Wurzeln der Kongruenz

$$X^\delta \equiv 1 \pmod{p, P(x)} \tag{146}$$

sind, welche nicht mehr als δ Wurzeln besitzt, so stellen sie die sämtlichen Wurzeln der letzteren dar; sie enthalten daher unter sich alle inkongruenten zum Exponenten δ gehörigen Funktionen, da auch diese der Kongruenz (146) genügen. Für irgend eine jener Potenzen, $f(x)^h$, sei d der Exponent, zu welchem sie (modd. p, $P(x)$) gehört; dann wird $f(x)^{hd} \equiv 1$ also hd durch δ teilbar sein; hieraus schliefst man leicht, dafs d dann und nur dann gleich δ sein wird, wenn h, δ relativ prim sind. Es giebt demnach $\varphi(\delta)$ unter den Potenzen (145) d. h. $\varphi(\delta)$ inkongruente Funktionen, welche (modd. p, $P(x)$) zum Teiler δ von $p^m - 1$ gehören, falls es überhaupt eine solche Funktion $f(x)$ giebt.

Sind aber $1, \delta', \delta'', \ldots p^m - 1$ die sämtlichen Teiler von $p^m - 1$, so verteilen sich alle Funktionen (modd. p, $P(x)$) in Gruppen, deren

Glieder resp. zu jenen Teilern als Exponenten gehören, und wenn $\chi(\delta)$ die Anzahl der Funktionen in der zum Teiler δ gehörigen Gruppe bezeichnet, so ist dem Bewiesenen zufolge entweder $\chi(\delta) = 0$ oder $\chi(\delta) = \varphi(\delta)$. Da indessen sowohl

$$\varphi(1) + \varphi(\delta') + \varphi(\delta'') + \cdots + \varphi(p^m - 1) = p^m - 1$$

als auch

$$\chi(1) + \chi(\delta') + \chi(\delta'') + \cdots + \chi(p^m - 1) = p^m - 1$$

sein mufs, erschliefst man, dafs stets $\chi(\delta) = \varphi(\delta)$ ist, und somit den Satz:

Zu jedem Teiler δ von $p^m - 1$ gehören (modd. p, $P(x)$) genau $\varphi(\delta)$ inkongruente Funktionen. Insbesondere giebt es daher $\varphi(p^m - 1)$ inkongruente primitive Wurzeln (modd. p, $P(x)$) d. h. solche Funktionen, welche zum Exponenten $p^m - 1$ gehören, und wenn $f(x)$ irgend eine solche ist, so sind die $p^m - 1$ Potenzen

$$(147) \qquad f(x),\ f(x)^2,\ f(x)^3, \ldots f(x)^{p^m - 1}$$

unter einander (modd. p, $P(x)$) inkongruent und stellen daher ein vollständiges reduziertes Restsystem nach diesem Doppelmodulus dar.

26. Ist insbesondere δ der Exponent, zu welchem x selbst (modd. p, $P(x)$) gehört, also $x^\delta - 1$ unter allen Ausdrücken von der Gestalt $x^h - 1$ derjenige niedrigsten Grades, der (mod. p) den Primteiler $P(x)$ hat, so ist, wie gezeigt, δ ein Teiler von $p^m - 1$, kann aber nicht Teiler eines Ausdrucks $p^n - 1$ von der gleichen Gestalt sein, in welchem $n < m$ ist, mit andern Worten: p gehört im gewöhnlichen zahlentheoretischen Sinne zum Exponenten m (mod. δ); denn, ginge im Gegenteil δ in $p^n - 1$ auf, so würde aus der vorausgesetzten Kongruenz

$$x^\delta - 1 \equiv 0 \text{ (modd. } p,\ P(x))$$

sich

$$x^{p^n - 1} - 1 \equiv 0 \text{ (modd. } p,\ P(x))$$

ergeben d. h. die Primfunktion $P(x)$ vom Grade m wäre (mod. p) ein Teiler von $x^{p^n} - x$, während $n < m$ ist, was gegen Nr. 23, 1) verstöfst. Bezeichnet man demgemäfs δ (mit Serret, Nr. 352) als einen dem Ausdrucke $p^m - 1$ eigenen Teiler, so darf man sagen: der Exponent, zu welchem x (modd. p, $P(x)$) gehört, ist ein dem Ausdrucke $p^m - 1$ eigener Teiler, wenn $P(x)$ eine Primfunktion m^{ten} Grades bezeichnet.

Umgekehrt sei jetzt δ eine beliebig gegebene zu p prime Zahl und die Zerlegung von

$$x^\delta - 1$$

in Primfunktionen (mod. p) zu ermitteln.*) Es gehöre p (mod. δ) zum Exponenten m, sodafs δ ein dem Ausdrucke $p^m - 1$ eigener Teiler ist. Jede Primfunktion $P(x)$ (mod. p), für welche x zum Exponenten δ gehört, wird ein Primteiler von $x^\delta - 1$ sein, dagegen keinem gleichgestalteten Ausdrucke $x^h - 1$ geringeren Grades als Teiler angehören und aus dieser Rücksicht ein primitiver Primteiler von $x^\delta - 1$ genannt werden dürfen. Ist ferner $\Pi(x)$ irgend ein irreduktibler Teiler dieses Ausdrucks, μ sein Grad und d der Exponent, zu welchem x (modd. p, $\Pi(x)$) gehört, also $x^d - 1$ der Ausdruck geringsten Grades, für welchen

$$x^d - 1 \equiv 0 \pmod{p,\ \Pi(x)}$$

ist, so ist notwendigerweise δ und daher auch $p^m - 1$ ein Vielfaches von d d. h. $p^m \equiv 1$ (mod. d), während p (mod. d) zum Exponenten μ gehört, mithin geht μ auf in m. Hieraus erschliefst man erstens, dafs d nur dann gleich δ sein kann, wenn $\mu = m$ ist, dafs also nur Primfunktionen m^{ten} Grades primitive Primteiler von $x^\delta - 1$ sein können. Zweitens, dafs jeder Primteiler dieses Ausdrucks ein primitiver Primteiler eines Ausdrucks $x^d - 1$ ist, bei welchem d ein Teiler von δ ist. Drittens leuchtet aber auch ein, dafs jeder Primteiler, insbesondere also auch jeder primitive Primteiler von $x^d - 1$, falls d irgend ein Teiler von δ ist, ein Primteiler von $x^\delta - 1$ sein mufs, da dieser Ausdruck algebraisch durch jenen teilbar ist. Da endlich $x^\delta - 1$ keine mehrfachen Teiler haben kann, indem der Gleichheit

$$x \cdot \delta x^{\delta - 1} - \delta \cdot (x^\delta - 1) = \delta$$

zufolge und weil δ nach Voraussetzung prim zu p ist, $x^\delta - 1$ und die Abgeleitete $\delta x^{\delta - 1}$ keinen (mod. p) gemeinsamen Teiler besitzen, so folgert man aus alle diesem, dafs die sämtlichen Primteiler von $x^\delta - 1$ (mod. p) mit den primitiven Primteilern aller Ausdrücke $x^d - 1$, in denen d gleich δ oder ein Teiler von δ ist, übereinstimmen und nachstehende Kongruenz bestehen mufs:

$$x^\delta - 1 \equiv \prod_d P^{(d)}(x) \pmod{p},$$

in welcher $P^{(d)}(x)$ das Produkt aller primitiven primären Primteiler von $x^d - 1$ bezeichnet. Aus dieser Kongruenz leitet

---

*) Es genügt, den Fall zu betrachten, in welchem δ prim ist gegen p. Denn, wäre $\delta = p^\alpha \cdot \delta'$, wo δ' nicht mehr teilbar durch p, so folgte

$$x^\delta - 1 = x^{p^\alpha \delta'} - 1 \equiv \left(x^{p^{\alpha - 1}\delta'} - 1\right)^p$$

und allgemeiner

$$x^\delta - 1 \equiv \left(x^{\delta'} - 1\right)^{p^\alpha} \pmod{p}$$

und die Zerlegung von $x^\delta - 1$ in irreduktible Faktoren ergäbe sich aus derjenigen von $x^{\delta'} - 1$.

sich aber, ganz wie die Formel (144) aus der Kongruenz (141) hervorging, die nachstehende Formel:

$$(148)\qquad P^{(\delta)}(x) \equiv \frac{(x^\delta - 1)\cdot \Pi\left(x^{\frac{\delta}{\alpha\beta}} - 1\right)\cdots}{\Pi\left(x^{\frac{\delta}{\alpha}} - 1\right)\cdot \Pi\left(x^{\frac{\delta}{\alpha\beta\gamma}} - 1\right)\cdots} \pmod{p},$$

in welcher $\alpha, \beta, \gamma, \ldots$ die verschiedenen Primfaktoren von δ sind, durch die Bemerkung her, daſs der Ausdruck zur Rechten bekanntlich eine ganze, ganzzahlige Funktion ist, was übrigens ähnlich zu erweisen ist, als es für die Funktion $F(x)$ in Nr. 23 geschehen ist.

Der Grad der rechten Seite von (148) ist

$$\delta - \sum \frac{\delta}{\alpha} + \sum \frac{\delta}{\alpha\beta} - \sum \frac{\delta}{\alpha\beta\gamma} + \cdots = \varphi(\delta);$$

gleich groſs ist folglich auch der Grad von $P^{(\delta)}(x)$ (mod. p) d. i. der Grad des Produktes aller primitiven Primteiler von $x^\delta - 1$ oder, was dasselbe war, aller Primfunktionen $P(x)$ m^{ten} Grades (mod. p), für welche x zum Exponenten δ gehört (oder, wie Serret umgekehrt sagt: welche zu dem Exponenten δ gehören); daher beträgt die Anzahl dieser Funktionen $P(x)$

$$\frac{\varphi(\delta)}{m}.$$

Hieraus folgert man einen früher in weiterem Umfange gefundenen zahlentheoretischen Satz, daſs nämlich der Exponent m, zu welchem eine zu δ prime Primzahl p gehört, ein Teiler von $\varphi(\delta)$ ist.

In dem besonderen Falle, wo δ eine Primzahl q ist, reduziert sich der vorige Ausdruck auf $\frac{q-1}{m}$ und die Kongruenz (148) nimmt die einfache Gestalt

$$P^{(q)}(x) \equiv \frac{x^q - 1}{x - 1} \pmod{p}$$

oder, wenn $\frac{q-1}{m} = n$ gesetzt und die n primären Primfunktionen m^{ten} Grades, für welche x zu dem, dem Ausdrucke $p^m - 1$ eigenen Teiler q als Exponenten gehört, mit $P_1(x), P_2(x), \ldots P_n(x)$ bezeichnet werden, die entwickeltere Gestalt:

$$(149)\qquad \frac{x^q - 1}{x - 1} \equiv P_1(x)\, P_2(x) \ldots P_n(x) \pmod{p}$$

an. Man erhält daher folgenden zuerst von Schönemann ausgesprochenen und hergeleiteten Satz: Ist q eine Primzahl, in Bezug auf welche die Primzahl p zum Exponenten m gehört, so ist $\frac{q-1}{m}$ eine ganze Zahl n (oder q von der Form $mn + 1$) und der Ausdruck $\frac{x^q - 1}{x - 1}$ zerfällt (mod. p) in ein Produkt aus n primären Primfunktionen vom Grade m.

Ist insbesondere die Primzahl p primitive Wurzel von q, also $m = q - 1$, $n = 1$, so ist die Funktion $\frac{x^q - 1}{x - 1}$ irreduktibel (mod. p).

Sei nun g irgend eine primitive Wurzel (mod. q); dann giebt es nach dem schon in Kap. 2, Nr. 7 erwähnten Dirichletschen Satze in der arithmetischen Progression $qz + g$ d. i. unter den mit g (mod. q) kongruenten Zahlen auch eine Primzahl p, welche daher ebenfalls primitive Wurzel (mod. q) ist. Weil der letzten Bemerkung zufolge in Bezug auf diese Primzahl p der Ausdruck $\frac{x^q - 1}{x - 1}$ irreduktibel ist, mufs er es a fortiori auch in algebraischem Sinne sein, und so liefert unsere Theorie nebenbei einen Beweis für die Irreduktibilität der Kreisteilungsgleichung, nämlich für den folgenden Satz: Die Gleichung

$$\frac{x^q - 1}{x - 1} = 0,$$

auf deren Lösung die Teilung einer Kreisperipherie in q gleiche Teile beruht, ist irreduktibel, so oft q eine Primzahl ist. (S. Ende der ersten der Schönemannschen Arbeiten.)

Ist ferner p eine Primzahl von der Form $qz + 1$, gehört also p zum Exponenten 1 (mod. q), so wird $n = q - 1$ und der obige allgemeine Satz besagt den besonderen, welcher folgt:

Für jede Primzahl p von der Form $qz + 1$ zerfällt der Ausdruck $\frac{x^q - 1}{x - 1}$ (mod. p) in ein Produkt aus $q - 1$ primären Funktionen ersten Grades und somit hat die Kongruenz

$$\frac{x^q - 1}{x - 1} \equiv 0 \pmod{p}$$

genau $q - 1$ ganzzahlige Wurzeln.

27. Wir kehren noch einmal zu der Kongruenz (141) oder zu dem Satze zurück, dafs die Funktion $x^{p^m} - x$ (mod. p) mit dem Produkte aller inkongruenten primären Primfunktionen der Grade μ, welche Teiler von m sind, identisch sei. Setzen wir das Zeichen X an Stelle von x, so kommt

$$X^{p^m} - X \equiv \prod_{\mu} \Phi_\mu(X) \pmod{p} \tag{150}$$

mithin auch (modd. p, $P(x)$), wo $P(x)$ irgend eine (mod. p) irreduktible Funktion sein kann, deren Grad wir gleich m wählen. Da alsdann nach dem Fermatschen Satze die Kongruenz

$$X^{p^m} - X \equiv 0 \quad (\text{modd. } p,\ P(x))$$

genau soviel Wurzeln hat, als ihr Grad beträgt, nämlich durch jede der p^m (modd. p, $P(x)$) inkongruenten Funktionen $f(x)$ befriedigt wird,

so müssen wegen (150) auch die einzelnen Primfunktionen, aus denen $X^{p^m} - X$ sich zusammensetzt, genau soviel Wurzeln haben, als ihr Grad beträgt. Hieraus folgt der Satz: Ist $P(x)$ eine (mod. p) irreduktible Funktion vom Grade m, μ ein Teiler von m und $P_\mu(x)$ eine beliebige der (mod. p) irreduktiblen Funktionen μ^{ten} Grades, so hat die Kongruenz

$$(151)\qquad P_\mu(X) \equiv 0 \text{ (modd. } p,\ P(x))$$

genau μ Wurzeln.

Der näheren Untersuchung dieser Wurzeln werde ein Hilfssatz vorangestellt, der Folgendes aussagt: Ist $F(X)$ eine ganze, ganzzahlige Funktion von X, so sind die sämtlichen Potenzen

$$(152)\qquad f(x),\ f(x)^p,\ f(x)^{p^2},\ f(x)^{p^3}, \ldots$$

Wurzeln der Kongruenz

$$(153)\qquad F(X) \equiv 0 \text{ (modd. } p,\ P(x))$$

wenn die ganze, ganzzahlige Funktion $f(x)$ eine Wurzel derselben ist. Denn alsdann besteht eine Gleichung von der Form:

$$F(f(x)) = p \cdot \varphi(x) + P(x) \cdot \psi(x),$$

in welcher auch $\varphi(x)$, $\psi(x)$ ganze und ganzzahlige Funktionen von x sind. Ersetzt man in ihr die Unbestimmte x durch x^p, so geht zunächst die andere Gleichung:

$$F(f(x^p)) = p \cdot \varphi(x^p) + P(x^p) \cdot \psi(x^p)$$

hervor. Nach (139) ist aber

$$f(x^p) \equiv f(x)^p, \quad P(x^p) \equiv P(x)^p \text{ (mod. } p),$$

und so nimmt offenbar die vorige Gleichung die neue Gestalt an:

$$F(f(x)^p) = p \cdot \varphi_1(x) + P(x)^p \cdot \psi_1(x),$$

in welcher wieder $\varphi_1(x)$, $\psi_1(x)$ ganze, ganzzahlige Funktionen sind, und welche als Kongruenz geschrieben werden kann, wie folgt:

$$F(f(x)^p) \equiv 0 \text{ (modd. } p,\ P(x));$$

mithin ist auch $f(x)^p$ und nun auch wieder $f(x)^{p^2}$, dann $f(x)^{p^3}$ u. s. f. eine Wurzel von (153), w. z. b. w.

Nun können aber die unendlich vielen Potenzen (152) nicht sämtlich inkongruent (modd. p, $P(x)$) sein, da es in Bezug auf diesen Doppelmodulus nur eine endliche Anzahl, nämlich, wenn $P(x)$ vom m^{ten} Grade ist (mod. p), p^m inkongruente Funktionen giebt. Daher mufs etwa

$$f(x)^{p^{\lambda+\mu}} \equiv f(x)^{p^\lambda} \text{ also auch } f(x)^{p^{m+\mu}} \equiv f(x)^{p^m}$$

und folglich nach dem Fermatschen Satze

$$f(x)^{p^\mu} \equiv f(x) \text{ (modd. } p,\ P(x))$$

sein. Ist $f(x)$ zu $P(x)$ prim (mod. p) und μ die kleinste aller Zahlen, für welche eine Kongruenz dieser Gestalt stattfindet, so ist leicht zu erkennen, dafs μ ein Teiler von m ist, denn aus dem gleichzeitigen Bestehen der Kongruenzen

$$f(x)^{p^\mu - 1} \equiv 1, \quad f(x)^{p^m - 1} \equiv 1$$

folgt auch $f(x)^d \equiv 1$, wenn d den gröfsten gemeinsamen Teiler von $p^m - 1$ und $p^\mu - 1$ bedeutet; der letztere aber ist $d = p^k - 1$, wenn k der gröfste gemeinsame Teiler von m und μ ist; in der That, ist d irgend ein gemeinsamer Teiler von $p^m - 1$ und $p^\mu - 1$, so ist $p^m \equiv 1$, $p^\mu \equiv 1$ also auch $p^k \equiv 1$ (mod. d), mithin d ein Teiler von $p^k - 1$; da aber $p^k - 1$ algebraisch aufgeht in $p^m - 1$, $p^\mu - 1$, ist es selbst ein gemeinsamer und daher der gröfste gemeinsame Teiler beider Differenzen. Danach erhielte man die Kongruenz $f(x)^{p^k - 1} \equiv 1$ oder

$$f(x)^{p^k} \equiv f(x) \text{ (modd. } p, \ P(x)),$$

in welcher, der Bedeutung der Zahl μ zuwider, $k < \mu$ sein würde, wenn nicht μ selbst der gröfste gemeinsame Teiler von m und μ d. h. ein Teiler von m wäre. Somit erhält man folgenden Satz:

Für jede (mod. p) zu $P(x)$ prime Funktion $f(x)$ giebt es einen kleinsten Exponenten μ so beschaffen, dafs

$$f(x)^{p^\mu} \equiv f(x) \text{ (modd. } p, \ P(x)) \tag{154}$$

ist, und dieser Exponent, welcher der Exponent genannt werden soll, zu welchem die Funktion $f(x)$ (modd. p, $P(x)$) pafst, ist stets ein Teiler von m.

Nunmehr überzeugt man sich sogleich, dafs dann die Potenzen

$$f(x), \ f(x)^p, \ f(x)^{p^2}, \ldots f(x)^{p^{\mu-1}} \tag{155}$$

(modd. p, $P(x)$) inkongruent sind, da sonst, wie vorher, eine Kongruenz von der Gestalt

$$f(x)^{p^k} \equiv f(x)$$

hervorgehen würde, in welcher $k < \mu$ wäre, gegen die Bedeutung von μ.

Nachdem dies festgestellt ist, betrachte man einen ganzen, ganzzahligen Ausdruck

$$S\left(f(x), \ f(x)^p, \ldots f(x)^{p^{\mu-1}}\right),$$

welcher aus den Gröfsen (155) symmetrisch zusammengesetzt ist. Bezeichnet man ihn, der auch in Bezug auf x eine ganze und ganzzahlige Funktion ist, als solche mit $S(x)$, so besteht die Kongruenz

$$S(x)^p \equiv S(x^p) \text{ (mod. } p)$$

d. h.
$$S(x)^p \equiv S\left(f(x^p), \ f(x^p)^p, \ldots f(x^p)^{p^{\mu-1}}\right)$$

eine Kongruenz, deren rechte Seite man mit Rücksicht auf (139) durch die kongruente Funktion

$$S(f(x)^p,\ f(x)^{p^2}, \dots f(x)^{p^\mu})$$

ersetzen darf; da aber die so (mod. p) nachgewiesene Kongruenz a fortiori (modd. p, $P(x)$) besteht, so darf mit Rücksicht auf (154) der letzte Ausdruck auch durch

$$S(f(x)^p,\ f(x)^{p^2}, \dots f(x))$$

d. h. wegen der vorausgesetzten Symmetrie des Ausdruckes S (das Gleiche erschlösse man auch für cyklische Funktionen der Elemente (155)) durch $S(x)$ ersetzt werden, und somit gelangt man zu folgender Kongruenz:

$$S(x)^p \equiv S(x) \ (\text{modd. } p,\ P(x)). \tag{156}$$

Nun hat die Kongruenz

$$X^p \equiv X \ (\text{modd. } p,\ P(x))$$

die p Wurzeln $X \equiv 0, 1, 2, \dots p-1$, denn diese erfüllen sogar die Kongruenz

$$X^p \equiv X \ (\text{mod. } p)$$

und sind, wie leicht zu sehen, auch (modd. p, $P(x)$) inkongruent. Auf Grund hiervon folgert man aus (156) den Satz: Paſst eine Funktion $f(x)$ (modd. p, $P(x)$) zum Exponenten μ, so ist jede ganze und ganzzahlige symmetrische Funktion der Potenzen (155) nach jenem Doppelmodulus einer ganzen Zahl kongruent.

Jene Potenzen sind demnach die Wurzeln einer ganzen, ganzzahligen Kongruenz

$$\psi(X) \equiv 0 \ (\text{modd. } p,\ P(x)) \tag{157}$$

vom Grade μ; denn, wählt man

$$\psi(X) \equiv (X - f(x)) \cdot (X - f(x)^p) \dots (X - f(x)^{p^{\mu-1}})$$

nämlich als diejenige ganzzahlige Funktion, deren Koeffizienten den symmetrischen Funktionen der Gröſsen (155), welche die Koeffizienten des entwickelten Produkts bilden, kongruent sind, so wird die Kongruenz (157) durch jede der Potenzen (155) erfüllt. Die Funktion $\psi(X)$ ist aber zudem irreduktibel (mod. p); wäre nämlich im Gegenteil

$$\psi(X) \equiv \varphi(X) \cdot \chi(X)$$

(mod. p) und also auch (modd. p, $P(x)$), wo $\varphi(X)$, $\chi(X)$ Faktoren geringeren Grades sind als $\psi(X)$, so hätte etwa die Kongruenz

$$\varphi(X) \equiv 0 \ (\text{modd. } p,\ P(x))$$

die Funktion $f(x)$ und folglich auch jede der Potenzen (155) zu Wurzeln, hätte also, was nicht sein kann, mehr Wurzeln, als ihr Grad

beträgt. Somit ist $\psi(X)$ notwendig eine der mit $P_\mu(X)$ bezeichneten Funktionen, und man darf sagen:

Pafst eine Funktion $f x)$ zum Exponenten μ, so sind die Potenzen (155) die Wurzeln einer der Kongruenzen (151):

$$P_\mu(X) \equiv 0 \text{ (modd. } p, P(x)).$$

Umgekehrt erkennt man aber sehr einfach, dafs jede Wurzel $f(x)$ einer beliebigen der Kongruenzen (151) nach dem Doppelmodulus $p, P(x)$ zum Exponenten μ pafst. Denn mit $f(x)$ zugleich werden die sämtlichen Potenzen (152) Wurzeln, folglich, wenn ν der Exponent wäre, zu welchem $f(x)$ pafst, die Potenzen

$$f(x), f(x)^p, f(x)^{p^2}, \ldots f(x)^{p^{\nu-1}} \tag{158}$$

ν inkongruente Wurzeln der vorigen Kongruenz, zugleich aber auch die Wurzeln der ganzzahligen Kongruenz

$$\psi(X) \equiv (X - f(x)) \cdot (X - f(x)^p) \ldots (X - f(x)^{p^{\nu-1}}) \equiv 0 \text{ (modd. } p, P(x)).$$

Es müfste also $\nu \overline{\overline{<}} \mu$ sein. Bildet man aber in der Weise der Nr. 19 eine Kongruenz

$$P_\mu(X) \equiv \psi(X) \cdot Q(X) + R(X)$$

(mod. p) also auch (modd. $p, P(x)$), so müfste $R(X) \equiv 0$ sein, da auch diese Funktion, welche von geringerem Grade ist als $\psi(X)$, durch die ν Potenzen (158) erfüllt wird; somit wäre

$$P_\mu(X) \equiv \psi(X) \cdot Q(X) \text{ (modd. } p, P(x))$$

und, da die Koeffizienten ganze Zahlen sind, auch (mod. p), d. h. $\psi(X)$ wäre ein Teiler der (mod. p) irreduktiblen Funktion $P_\mu(x)$ also identisch mit ihr; mithin mufs $\nu = \mu$ sein, wie behauptet.

Die beiden letzten Sätze lassen erkennen, dafs die sämtlichen Funktionen $f(x)$, welche zum Exponenten μ passen, mit den Wurzeln aller (μ) (mod. p) irreduktibeln Kongruenzen $P_\mu(X) \equiv 0$ vom Grade μ identisch sind. Da nun jede solche Kongruenz, (modd. $p, P(x)$) aufgefafst, μ jener Funktionen zu Wurzeln hat, ein- und dieselbe Funktion $f(x)$ aber nicht zwei verschiedenen Kongruenzen $P_\mu'(X) \equiv 0$, $P_\mu''(X) \equiv 0$ genügen kann, da diese sonst die ganze Reihe der Potenzen (155) zu Wurzeln d. h. sämtliche Wurzeln gemeinsam haben und folglich die Funktionen $P_\mu'(X)$, $P_\mu''(X)$ auch (mod. p) übereinstimmen würden, so beträgt die gesamte Anzahl aller zu einem beliebigen Teiler μ von m passenden Funktionen

$$\mu \cdot (\mu). \tag{159}$$

Hatten wir also früher gefunden, dafs jede (mod. p) zu $P(x)$ prime Funktion $f(x)$ zu einem bestimmten Teiler μ von m pafst, so hat sich nunmehr herausgestellt, dafs es auch für jeden Teiler μ von m passende Funktionen dieser Art giebt, und wie grofs deren Anzahl. —

Wendet man die für die Funktionen $P_\mu(X)$ gefundenen Sätze speziell auf die Kongruenz

$$(160) \qquad P(X) \equiv 0 \pmod{p, P(x)}$$

vom Grade m an, für welche offenbar $X \equiv x$ eine Wurzel ist, so kommt man zu folgenden Ergebnissen:

Die Gröfse x pafst (modd. p, $P(x)$) zum Exponenten m, d. h., während

$$x^{p^m} \equiv x \pmod{p, P(x)}$$

ist, sind die Potenzen

$$(161) \qquad x, x^p, x^{p^2}, \ldots x^{p^{m-1}}$$

nach diesem Doppelmodulus inkongruent und bilden die sämtlichen Wurzeln der Kongruenz (160). Ganze und ganzzahlige, symmetrische Funktionen der Potenzen (161) sind ganzen Zahlen kongruent.

Da somit auch die Kongruenz

$$P(X) - (X-x)(X-x^p)\ldots(X-x^{p^{m-1}}) \equiv 0$$

durch die m Potenzen (161) erfüllt wird, so ist identisch

$$(162) \quad P(X) \equiv (X-x)(X-x^p)\ldots(X-x^{p^{m-1}}) \pmod{p, P(x)},$$

ein Resultat, welches schon bei Schoenemann § 18 gefunden wird. Mit andern Worten: Ist:

$$P(X) = X^m + A_1X^{m-1} + \cdots + A_{m-1}X + A_m,$$

so ist $-A_1$ der Summe aller Gröfsen (161), A_2 der Summe aller ihrer Kombinationen zu je zwei, $-A_3$ der Summe ihrer Kombinationen zu je drei u. s. w., endlich $(-1)^m A_m$ ihrem Produkte (modd. p, $P(x)$) kongruent, wie Gaufs Nr. 357 dasselbe Resultat ausgedrückt hat.

Wir beschliefsen die Betrachtungen dieser Nr. mit dem Beweise des folgenden allgemeinen und besonders wichtigen Satzes:

Ist $F(X)$ eine ganze ganzzahlige Funktion von X n^{ten} Grades (mod. p), so läfst sich stets eine (mod. p) irreduktible Funktion $P(x)$ angeben, so beschaffen, dafs die Kongruenz

$$(163) \qquad F(X) \equiv 0 \pmod{p, P(x)}$$

genau n (gleiche oder ungleiche) Wurzeln hat.

In der That, sei — (mod. p) in primäre Primfunktionen zerlegt —

$$(164) \qquad F(X) \equiv P_{\mu_1}(X)^{a_1} \cdot P_{\mu_2}(X)^{a_2} \ldots \pmod{p}$$

und seien $\mu_1, \mu_2, \mu_3, \ldots$ die Grade der unter einander verschiedenen Primteiler, m aber ihr kleinstes gemeinsames Vielfaches. Ist dann $P(x)$ irgend eine (mod. p) irreduktible Funktion m^{ten} Grades, wie es deren nach Nr. 21 stets giebt, so hat jede der Kongruenzen

$$(165) \qquad P_{\mu_1}(X) \equiv 0, \quad P_{\mu_2}(X) \equiv 0, \ldots \pmod{p, P(x)}$$

nach dem in dieser Nr. Bewiesenen genau soviel Wurzeln, sämtlich von der Form $f(x)$, als ihr Grad beträgt, auch kann ersichtlich nicht ein- und dieselbe Funktion $f(x)$ zwei verschiedenen dieser irreduktibeln Kongruenzen genügen. Da aber aus (164) auch

$$(166) \qquad F(X) \equiv P_{\mu_1}(X)^{a_1} \cdot P_{\mu_2}(X)^{a_2} \dots (\text{modd. } p,\ P(x))$$

folgt, so hat die Kongruenz (163) alle Wurzeln der Kongruenzen (165) ebenfalls, jede derselben resp. $a_1, a_2, a_3, \dots$ Mal, also, da $a_1\mu_1 + a_2\mu_2 + \dots = n$ sein mufs, mindestens n gleiche oder verschiedene Wurzeln. Andererseits mufs jede Wurzel der Kongruenz (163) wegen (166) einer der Kongruenzen (165) genügen, also kann jene keine andern als die bezeichneten Wurzeln besitzen und hat also deren genau n. Man findet nämlich identisch:

$$F(X) \equiv \prod (X - f_1(x))^{a_1} \cdot \prod (X - f_2(x))^{a_2} \dots (\text{modd. } p,\ P(x)),$$

wenn hier die einzelnen Produkte je auf die verschiedenen Wurzeln der Kongruenzen (165) resp. erstreckt werden.

28. Die Sätze der vorigen Nr. nehmen einen einfacheren und sehr eleganten Ausdruck an, wenn man sich der sogenannten „Galoisschen Imaginären“ bedient. Zu diesen gelangt man durch die einfache Überlegung, dafs, wenn $P(x)$ eine (mod. p) irreduktible Funktion vom Grade $m > 1$ ist, die Kongruenz

$$(167) \qquad P(x) \equiv 0 \ (\text{mod. } p)$$

zwar keine ganzzahligen Wurzeln zuläfst, dafs man aber eine „Imaginäre i“ denken oder definieren kann, welche die Kongruenz

$$(168) \qquad P(i) \equiv 0 \ (\text{mod. } p)$$

erfüllt; man darf z. B. unter i irgend eine Wurzel α der irreduktibeln Gleichung $P(x) = 0$ verstehen. Besteht nun die Kongruenz

$$(169) \qquad f_1(x) \equiv f_2(x) \ (\text{modd. } p,\ P(x))$$

d. h. eine Gleichung von der Form

$$f_1(x) = f_2(x) + p \cdot \varphi(x) + P(x) \cdot \psi(x),$$

so folgt daraus mit Rücksicht auf die Definition von i

$$(170) \qquad f_1(i) \equiv f_2(i) \ (\text{mod. } p).$$

Umgekehrt aber hätten, wenn diese Kongruenz erfüllt ist, die beiden Kongruenzen

$$f_1(x) - f_2(x) \equiv 0, \quad P(x) \equiv 0 \ (\text{mod. } p)$$

die gemeinsame Lösung i und demnach die Funktionen $f_1(x) - f_2(x)$, $P(x)$ einen (mod. p) gemeinsamen Teiler, der, weil $P(x)$ irreduktibel ist, nur $P(x)$ selbst sein kann; es müfste mithin $f_1(x) - f_2(x)$ (mod. p) teilbar sein durch $P(x)$ und somit folgt aus dem Stattfinden

der Kongruenz (170) wieder rückwärts die Kongruenz (169). Demnach sind beide Kongruenzen völlig äquivalent.

Insbesondere wird also eine ganze, ganzzahlige Funktion $f(i)$ dann und nur dann (mod. p) kongruent Null sein, wenn $f(x) \equiv 0$ (modd. p, $P(x)$) ist. Da ferner für jede ganze, ganzzahlige Funktion $f(x)$ eine Kongruenz besteht:

$$f(x) \equiv \alpha_1 x^{m-1} + \alpha_2 x^{m-2} + \cdots + \alpha_m \text{ (modd. } p,\ P(x)),$$

wo die Koeffizienten ganze Zahlen $< p$ sind; so findet man allgemein

$$(171) \qquad f(i) \equiv \alpha_1 i^{m-1} + \alpha_2 i^{m-2} + \cdots + \alpha_m \text{ (mod. } p),$$

und aus dem Fermatschen Satze (133) ergiebt sich die Kongruenz

$$f(i)^{p^m} \equiv f(i) \text{ (mod. } p)$$

d. h. folgende einfachere Fassung jenes Satzes: Jede der p^m inkongruenten ganzen, ganzzahligen Funktionen (171) ist eine Wurzel der Kongruenz

$$(172) \qquad X^{p^m} \equiv X \text{ (mod. } p),$$

welche demnach genau soviel Wurzeln von der Form $f(i)$ zuläfst, als ihr Grad beträgt.

Da ferner aus jeder Lösung $f(x)$ der Kongruenz $F(X) \equiv 0$ (modd. p, $P(x)$) d. h. aus der Kongruenz

$$F(f(x)) \equiv 0 \text{ (modd. } p,\ P(x))$$

die andere: $F(f(i)) \equiv 0$ (mod. p) also eine Lösung $f(i)$ der Kongruenz $F(X) \equiv 0$ (mod. p) hervorgeht und umgekehrt, und da zwei Lösungen $f_1(x)$, $f_2(x)$ kongruent oder inkongruent sind (modd. p, $P(x)$), jenachdem $f_1(i)$, $f_2(i)$ es (mod. p) resp. sind, so schliefst man aus dem allgemeinen Satze der Nr. 22 den einfacheren Ausspruch: Eine Kongruenz $F(X) \equiv 0$ (mod. p) kann nicht mehr Wurzeln von der Form $f(i)$ haben, als ihr Grad beträgt.

In gleicher Weise übertragen sich die übrigen der in den vorigen Nrn. gefundenen Sätze in ihre neue Form. So erkennt man aus dem ersten Satze in Nr. 25, dafs jede Funktion $f(i)$ (mod. p) zu einem Exponenten gehört, der ein Teiler ist von $p^m - 1$; aus dem zweiten Satze derselben Nr., dafs zu jedem Teiler δ von $p^m - 1$ genau $\varphi(\delta)$ der Funktionen (171) gehören und dafs es folglich insbesondere $\varphi(p^m - 1)$ primitive Wurzeln der Kongruenz (172) von der Form $f(i)$ giebt. Ist $f(i)$ eine solche, so repräsentieren die Potenzen

$$f(i),\ f(i)^2,\ f(i)^3,\ \ldots\ f(i)^{p^m - 1}$$

sämtliche Funktionen (171) mit Ausnahme der einzigen, welche kongruent Null ist (mod. p).

Desgleichen schliefst man jetzt aus dem, was in Nr. 27 über die Kongruenz (151) gelehrt worden ist, dafs jede Kongruenz

$$P_\mu(X) \equiv 0 \pmod{p},$$

in welcher $P_\mu(x)$ eine (mod. p) irreduktible Funktion von einem in m aufgehenden Grade μ ist, genau μ Wurzeln von der Form $f(i)$ besitzt. Ist $f(i)$ eine solche, so sind die Potenzen

$$f(i),\ f(i)^p,\ f(i)^{p^2},\ \ldots\ f(i)^{p^{\mu-1}}$$

ihre sämtlichen Wurzeln. Ganze, ganzzahlige und symmetrische Funktionen dieser Potenzen sind (mod. p) ganzen Zahlen kongruent.

Insbesondere sind die Wurzeln der Kongruenz

$$P(X) \equiv 0 \pmod{p}$$

die Potenzen $i,\ i^p,\ i^{p^2},\ \ldots\ i^{p^{m-1}}$.

Der Schlufssatz endlich der vorigen Nr. erhält folgende neue Gestalt, aus der seine grofse Bedeutung deutlicher erkennbar wird: Ist $F(X)$ eine ganze, ganzzahlige Funktion von X vom Grade n (mod. p), so hat die Kongruenz

$$F(X) \equiv 0 \pmod{p}$$

immer genau n (gleiche oder verschiedene) Wurzeln, und zwar sind sie ganze und ganzzahlige Funktionen von der Gestalt (171), während i eine imaginäre Wurzel der in jenem Schlufssatze näher bestimmten (mod. p) irreduktibeln Funktion $P(x)$ vom Grade m bedeutet.

Die Einführung dieser Imaginären verdankt man Galois, der in einer zuerst im *Bulletin de Férussac* 13, 1830, p. 398 veröffentlichten und später im *Journ. de Math.* 11, 1846 reproduzierten Arbeit sie der Theorie der höheren Kongruenzen zu Grunde gelegt hat; aber auch Schoenemann's Darstellung dieser Theorie, der jene Galoissche Arbeit nicht gekannt haben dürfte, beruht kraft der Definitionen in § 14 seiner Abhandlung auf dem gleichen Gedanken, dem sogar in § 31 derselben noch allgemeinere Entwicklung gegeben wird.

29. Zum Schlusse liefern wir noch auf Grund dieser Betrachtungen den siebenten Gaufsschen Beweis des quadratischen Reziprozitätsgesetzes (Gaufs Nr. 365), obwohl wir eigentlich das Gebiet der Niederen Zahlentheorie damit überschreiten. Nach dem in Nr. 26 gegebenen Schoenemannschen Satze besteht, wenn q eine Primzahl bedeutet, in Bezug auf welche die Primzahl p zum Exponenten m gehört, die folgende Kongruenz:

$$\frac{X^q - 1}{X - 1} \equiv P_1(X)\, P_2(X) \ldots P_n(X) \pmod{p}, \tag{173}$$

worin $n = \frac{q-1}{m}$ ist und die n Faktoren zur Rechten (mod. p) irreduktible Funktionen m^{ten} Grades bedeuten. Demgemäfs wird, welche

(mod. p) irreduktible Funktion immer unter $P(x)$ verstanden werde, auch

(174) $$\frac{X^q - 1}{X - 1} \equiv P_1(X)\, P_2(X) \ldots P_n(X) \pmod{p,\, P(x)}$$

sein. Wird nun z. B. $P(x) = P_1(x)$ gewählt und unter i eine imaginäre Wurzel der Kongruenz

(175) $$P_1(x) \equiv 0 \pmod{p}$$

verstanden, so geht offenbar aus der Kongruenz (174) für $X = i$ die neue:

$$\frac{i^q - 1}{i - 1} \equiv 0 \pmod{p}$$

also auch $i^q \equiv 1 \pmod{p}$ hervor. Demnach sind offenbar die Potenzen

(176) $$i,\ i^2,\ i^3,\ \ldots\ i^{q-1}$$

sämtlich Wurzeln der Kongruenz $X^q \equiv 1 \pmod{p}$, zugleich aber auch unter einander inkongruent, denn sonst müfste eine gewisse Potenz i^h, wo $h < q$, der Einheit kongruent sein, und aus $i^q \equiv 1$ und $i^h \equiv 1$ dann auch $i \equiv 1$ folgen, gegen die Bedeutung von i. Man erkennt so, dafs alle Potenzen (176) Wurzeln der Kongruenz

(177) $$\frac{X^q - 1}{X - 1} \equiv 0 \pmod{p}$$

und ihre sämtlichen Wurzeln sein müssen. Sei nun g eine primitive Wurzel (mod. q); dann lassen sich jene Potenzen mit Rücksicht auf $i^q \equiv 1 \pmod{p}$ auch durch die folgende Reihe:

(178) $$i,\ i^g,\ i^{g^2},\ \ldots\ i^{g^{q-2}}$$

ersetzen; ferner ist für einen gewissen Exponenten π

$$p \equiv g^\pi \pmod{q};$$

da aber p (mod. q) zum Exponenten m gehört, mufs $m\pi$ das kleinste Vielfache von π sein, welches durch $q - 1 = mn$ teilbar wird, also findet sich $\pi = \lambda n$ und λ prim zu m. Man zerlege jetzt, ganz wie in der Theorie der Kreisteilung, die Reihe der Potenzen (178) auf folgende Weise in Gruppen, die sich wegen $p \equiv g^{\lambda n} \pmod{q}$ nach ihren in passender Folge genommenen Vertikalreihen aneinanderschliefsen:

(179) $$\left\{\begin{array}{l} i,\ \ i^p,\ \ i^{p^2},\ \ \ldots\ i^{p^{m-1}} \\ i^g,\ \ i^{gp},\ \ i^{gp^2},\ \ldots\ i^{gp^{m-1}} \\ i^{g^2},\ \ i^{g^2p},\ \ i^{g^2p^2},\ \ldots\ i^{g^2p^{m-1}} \\ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot \\ i^{g^{n-1}},\ \ i^{g^{n-1}p},\ \ldots\ i^{g^{n-1}p^{m-1}}, \end{array}\right.$$

bei welcher Zerlegung immer die Glieder einer jeden Gruppe aus dem ersten derselben hervorgehen, indem man dieses zur p^{ten}, $p^{2\text{ten}}$, ... $p^{m-1\,\text{ten}}$ Potenz erhebt. Da alle Potenzen (179) oder (178) die Kon-

gruenz (177) erfüllen, verteilen sie sich nach der Formel (173) auf die einzelnen Faktoren $P_1(X)$, $P_2(X)$, ... $P_n(X)$, und zwar sind die Glieder der ersten Gruppe, da i selbst eine Wurzel der Kongruenz (175) ist, deren sämtliche Wurzeln; ist also i^g etwa eine Wurzel der Kongruenz $P_2(X) \equiv 0 \pmod{p}$, so werden die Glieder der zweiten Gruppe sämtliche Wurzeln derselben Kongruenz sein; die der dritten Gruppe ergeben sich als sämtliche Wurzeln etwa der Kongruenz $P_3(X) \equiv 0 \pmod{p}$, u. s. w. Aus diesem Umstande folgt aber, dafs jede der symmetrisch aus jenen Wurzeln resp. gebildeten Summen:

$$\begin{aligned}
S_0 &= i + i^p + i^{p^2} + \cdots + i^{p^{m-1}} \\
S_1 &= i^g + i^{gp} + i^{gp^2} + \cdots + i^{gp^{m-1}} \\
S_2 &= i^{g^2} + i^{g^2p} + i^{g^2p^2} + \cdots + i^{g^2p^{m-1}} \\
&\cdots\cdots\cdots\cdots\cdots \\
S_{n-1} &= i^{g^{n-1}} + i^{g^{n-1}p} + \cdots + i^{g^{n-1}p^{m-1}}
\end{aligned}$$

nach dem Modulus p ganzen Zahlen kongruent sind.

Nunmehr werde angenommen, dafs p quadratischer Rest sei von q, also der Kongruenz $p^{\frac{q-1}{2}} \equiv 1 \pmod{q}$ genüge. Da nach der früheren Annahme $p \pmod{q}$ zum Exponenten m gehört, mufs dann $\frac{q-1}{2}$ durch m teilbar, also $n = \frac{q-1}{m}$ eine gerade Zahl sein. Alsdann werden die beiden Ausdrücke

$$\begin{aligned}
S(i) &= i + i^{g^2} + i^{g^4} + \cdots + i^{g^{q-3}}, \\
S_1(i) &= i^g + i^{g^3} + i^{g^5} + \cdots + i^{g^{q-2}},
\end{aligned}$$

welche den sogenannten zwei $\frac{q-1}{2}$-gliedrigen Perioden der Kreisteilungsgleichung entsprechen, resp. gleich

$$\begin{aligned}
&S_0 + S_2 + \cdots + S_{n-2}, \\
&S_1 + S_3 + \cdots + S_{n-1},
\end{aligned}$$

also $\pmod{p}$ ganzen Zahlen kongruent sein. Bildet man aber, ganz wie in der Theorie der Kreisteilung die Gleichung, welche jene Perioden zu Wurzeln hat, die Kongruenz $\pmod{p}$, der jene beiden Ausdrücke Genüge leisten, so findet man dafür die Kongruenz

$$X^2 + X + \frac{1 - (-1)^{\frac{q-1}{2}} \cdot q}{4} \equiv 0 \pmod{p}.$$

Diese hat also, wenn p quadratischer Rest $\pmod{q}$ ist, zwei ganzzahlige Wurzeln. Dasselbe gilt daher auch für die Kongruenz

$$(2X + 1)^2 \equiv (-1)^{\frac{q-1}{2}} \cdot q \pmod{p},$$

welche durch Multiplikation mit 4 aus jener entsteht. Ist also p quadratischer Rest von q, so ist $(-1)^{\frac{q-1}{2}} \cdot q$ quadratischer Rest von p, oder:

$$\text{aus } \left(\frac{p}{q}\right) = 1 \text{ folgt } (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{q}{p}\right) = 1.$$

Dies ist, was Gaufs a. a. O. beweist. Es genügt jedoch noch nicht zu einer vollständigen Begründung (*completa demonstratio, art.* 366) des Reziprozitätsgesetzes; für eine solche bedarf es vielmehr noch einer Ergänzung, die wir nun folgen lassen.

Wird nämlich jetzt p als quadratischer Nichtrest (mod. q) angenommen, sodafs $p^{\frac{q-1}{2}} \equiv -1$ (mod. q), so kann $\frac{q-1}{2}$ nicht durch m teilbar, und somit mufs $n = \frac{q-1}{m}$ ungerade sein. Man überzeugt sich in diesem Falle, in welchem m gerade also λ ungerade sein mufs, sogleich von der Richtigkeit der Kongruenzen

$$S(i^p) \equiv S_1(i), \quad S_1(i^p) \equiv S(i) \ \ (\text{mod. } p),$$

aus denen die Relation

$$S(i^p) - S_1(i^p) \equiv S_1(i) - S(i)$$

oder auch einfacher

$$(S(i) - S_1(i))^p \equiv -(S(i) - S_1(i))$$

hervorgeht. Aber ganz mit denselben Mitteln wie die Gaufssche Kreisteilungstheorie gelangt man zu der anderen Kongruenz:

$$(S(i) - S_1(i))^2 \equiv (-1)^{\frac{q-1}{2}} \cdot q \ \ (\text{mod. } p).$$

Man darf daher die voraufgehende Kongruenz durch $S(i) - S_1(i)$ dividieren und findet dann mit Rücksicht auf die letzte das Resultat:

$$(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot q^{\frac{p-1}{2}} \equiv -1 \ \ (\text{mod. } p).$$

$$\text{Aus } \left(\frac{p}{q}\right) = -1 \text{ folgt also } (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{q}{p}\right) = -1.$$

Immer ist daher

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{q}{p}\right),$$

d. h. es besteht das Reziprozitätsgesetz. —

Zusätze.

Zu Seite 34.

Beim Satze I mag man bemerken, dafs der Modulus, den wir (nz) nennen, mit der Reihe (1) nicht identisch zu sein braucht; denn, obwohl er alle Zahlen derselben enthält, könnte er sehr wohl Zahlen dieser Reihe mehrfach enthalten. Ähnliches gilt mit Bezug auf Satz II.

Zu Seite 50, Ende von Nr. 9.

Hier ist eine Ergänzung erforderlich. Nennt man $p, \ldots$ diejenigen Primzahlen, für welche die höchste vorhandene Potenz $p^\varepsilon, \ldots$ in m, dagegen $q, \ldots$ diejenigen, für welche die höchste vorhandene Potenz $q^\delta, \ldots$ in m' auftritt, endlich $r, \ldots$ diejenigen, die sich in m und m' zu gleich hoher Potenz $r^\gamma, \ldots$ erhoben finden, so wird

$$M = \prod (p^\varepsilon) \cdot \prod (q^\delta) \cdot \prod (r^\gamma)$$

sein und jede Zerlegung $M = \mu\mu'$ von der gedachten Art erhalten, wenn man setzt

$$\mu = \prod (p^\varepsilon) \cdot \prod{}' (r^\gamma), \quad \mu' = \prod (q^\delta) \cdot \prod{}'' (r^\gamma),$$

indem man die Primzahlpotenzen $r^\gamma \ldots$ in beliebiger Weise auf zwei Produkte Π', Π'' verteilt. Wenn nun alle Primzahlen in einer der Zahlen m, m' zu niedrigerer Potenz erhoben sind, als in der anderen, was nur eintreten kann, wenn die erstere ein Teiler der letzteren ist, so ist die einzige Zerlegung von M der gedachten Art die Zerlegung in die beiden Faktoren $1, M$; in jedem andern Falle kann man beide Zahlen μ, μ' von 1 verschieden wählen. Dies beachte man auf Seite 342.

Zu Seite 64.

Die von Landau angegebene Bedingung bezieht sich auf alle y_i zwischen 0 und 1 inklusive der Grenzen. Dafs aber die Ungleichheit (64) stattfindet, wenn eine der Gröfsen y_1, y_2 oder beide mit einer dieser Grenzen zusammenfallen, sowie auch dann, wenn sie einander gleich sind, versteht sich ohne weiteres. Hiernach bleiben, wie leicht zu übersehen, in der That nur die fünf unterschiedenen Fälle zu betrachten.

Zu Seite 111.

Die behauptete Symmetrie des Kettenbruchs (3) tritt, dem Beweise zufolge, selbstverständlich nur dann ein, wenn man eventuell den letzten Teilbruch $\frac{1}{q_k}$ durch $\cfrac{1}{(q_k - 1) + \cfrac{1}{1}}$ ersetzt.

Zu Seite 132.

Um jedem etwaigen Bedenken gegen das im Anschlufs an Serret's Handbuch der höheren Algebra angestellte Räsonnement zu begegnen,

sei hier noch nachgewiesen, dafs $\frac{Y_h}{Y_{h-1}}$ nicht mit unendlich wachsendem h gegen 1 konvergieren kann. Dies ist klar, wenn nur in dem Kettenbruche für w von keiner Stelle an die Teilnenner dauernd gleich 1 bleiben; denn, wählt man dann das hinreichend grofse h so, dafs $q_{h-1} > 1$ ist, so wird

$$\frac{Y_h}{Y_{h-1}} = q_{h-1} + \frac{Y_{h-2}}{Y_{h-1}} > 2.$$

Wenn aber von einer bestimmten Stelle an der Teilnenner dauernd gleich 1 bleibt, so gilt Folgendes. Tritt dieser Umstand von der h^{ten} Stelle an ein und heifst w_1 der entsprechende Schlufsteil des Kettenbruchs w, so ist (nach p. 116) $w_1 = \frac{1+\sqrt{5}}{2}$ und $\frac{g_i}{g_{i-1}}$ der i^{te} Näherungsbruch von w_1. Man findet daher

$$\frac{X_{h+i}}{Y_{h+i}} = \frac{g_i X_h + g_{i-1} X_{h-1}}{g_i Y_h + g_{i-1} Y_{h-1}}$$

und, da (wegen $g_0 = 1$) g_i, g_{i-1} relativ prim sind, sind Zähler und Nenner des letzteren Bruches, wie die des ersteren, teilerfremd, mithin

$$Y_{h+i} = g_i Y_h + g_{i-1} Y_{h-1}$$

also

$$\frac{Y_{h+i}}{Y_{h+i-1}} = \frac{g_i Y_h + g_{i-1} Y_{h-1}}{g_{i-1} Y_h + g_{i-2} Y_{h-1}} = \frac{Y_h \cdot \frac{g_i}{g_{i-1}} + Y_{h-1}}{Y_h + \frac{g_{i-2}}{g_{i-1}} Y_{h-1}},$$

ein Ausdruck, der mit unendlich wachsendem i den Wert

$$\frac{Y_h \cdot w_1 + Y_{h-1}}{Y_h + \frac{1}{w_1} Y_{h-1}} = w_1 > \frac{3}{2}$$

zur Grenze hat.

Zu Seite 146, Ende von Nr. 18.

Hier sei erläuternd hinzugefügt, dafs, wenn in einer Entwicklungsreihe zwei gleiche Gruppen a, b vorkämen, nur zwei Fälle möglich wären. Entweder stünden dieselben neben einander, bildeten mithin die Gruppe a, b, a, b; dann würde, jenachdem a oder b das Summenglied wäre, in der voraufgehenden Reihe die Gruppe b, b oder a, a auftreten, was, da zwei aufeinanderfolgende Glieder einer Reihe relativ prim sind, nur geschehen könnte, wenn sie die Gruppe 1, 1, also die gedachte Reihe die anfängliche Reihe wäre; von dieser ausgehend findet man aber in der nächsten Reihe keine doppelt vorhandene Gruppe. Oder die beiden Gruppen a, b wären in der Reihe, in welcher sie auftreten, getrennt; dann würden, wenn etwa wieder a

als Summenglied gedacht wird, in der voraufgehenden Reihe zwei gleiche Gruppen β, b auftreten, u. s. w., und man käme notwendig entweder zu dem vorigen unzulässigen Falle wieder zurück, oder auf eine Reihe, in welcher eine Gruppe $1, c$ oder $c, 1$ doppelt aufträte, was nicht geschehen kann.

Zu Seite 204, Chronologische Tabelle der Beweise des Reziprozitätsgesetzes.

Erst während des Druckes dieses Werkes wurde der Verfasser durch Herrn Edm. Landau mit zwei weiteren Beweisen bekannt: demjenigen von J. König (*Acta math.* 22, p. 181), der jedoch schon in der Begründung seines ersten Satzes eine wesentliche Lücke hat, durch welche er hinfällig wird, sowie demjenigen von E. Fischer (*Monatshefte für Math. u. Phys.*, 11. Jahrg., p. 176). Der letztere, zwar nicht in den Rahmen dieses Buches passende Beweis leitet, ausgehend von Eisenstein's (*application de l'algèbre à l'arithmétique transcendante*, Tabelle Nr. 13) Darstellung des Legendreschen Symbols als Resultante zweier ganzen Funktionen einer Veränderlichen, das Reziprozitätsgesetz allein mit Hilfe des Eulerschen Kriteriums direkt durch die Theorie solcher Resultanten her.

Zu Seite 224.

Bei dem Eisensteinschen Beweise bemerke man, dafs die in der Figur ebenfalls als Sternchen gezeichneten, auf den Axen liegenden Punkte in der Summation nicht mitrechnen.

Zu Seite 333.

Der Satz 2) und sein Beweis ist zu berichtigen, der Satz nämlich auf die Voraussetzung, dafs der Exponent δ ein Teiler von $p-1$ sei, und auf den Modulus p^α zu beschränken. Da dann die Primzahlen q, q_i von p verschieden sind, so finden sich in der That, wie einfach zu übersehen ist, die Kongruenzen

$$\frac{z^\delta - 1}{z^{\frac{\delta}{q}} - 1} \equiv 0 \quad \text{sowie} \quad \frac{z^\delta - 1}{z^{\delta_i} - 1} \equiv 0 \pmod{p^\alpha},$$

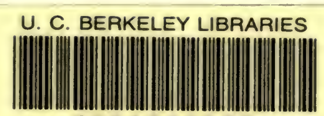
auf denen der Beweis beruht. — Übrigens gilt bei der, dem Exponenten δ jetzt auferlegten Beschränkung der erste auf den Fall, wo δ einen mehrfachen Primfaktor hat, bezügliche Teil des Satzes auch (mod. $2p^\alpha$). Denn, da alsdann z ungerade ist, so wird die auf alle Zahlen k, deren Anzahl $\varphi(\delta)$, also gerade ist, bezogene Summe Σz^k eine gerade Zahl und, da sie $\equiv 0$ (mod. p^α) gefunden wurde, auch $\equiv 0$ (mod. $2p^\alpha$) sein. — Dagegen gilt von dem auf S. 335 gefolgerten Satze nur der auf den einfachsten Fall eines Primzahlmodulus bezügliche Teil, nämlich der Satz von Gaufs.

Zu Seite 346. Lies auf Zeile 5 v. u. „nicht teilbar oder teilbar" statt „teilbar oder nicht teilbar".








U. C. BERKELEY LIBRARIES
C058585199





